# Chapter 4. Finite Fields

**Table of Contents**



The origins and history of finite fields can be traced back to the 17th and 18th centuries, but there, these fields played only a minor role in the mathematics of the day. In more recent times, however, finite fields have assumed a much more fundamental role and in fact are of rapidly increasing importance because of practical applications in a wide variety of areas such as coding theory, cryptography, algebraic geometry and number theory.

# Groups, Modular Arithmetic and Finite Fields

The structure of a finite field is a bit complex. So instead of introducing finite fields directly, we first have a look at another algebraic structure: groups. A group is a non-empty set (finite or infinite) $G$ with a binary operator • such that the following four properties (**Cain**) are satisfied:

- **C**losure: if $a$ and $b$ belong to $G$, then $a•b$ also belongs to $G$;
- **A**ssociative: $a•(b•c)=(a•b)•c$ for all $a, b, c$ in $G$;
- **I**dentity element: there is an element $e$ in $G$ such that $a•e = e•a = a$ for every element $a$ in $G$;
- **In**verse element: for every element $a$ in $G$, there's an element a' such that $a•a' = e$ where $e$ is the identity element.

We usually denote a group by ($G$, •) or simply $G$ when the operator is clear in the context. In general, a group is not necessarily commutative, i.e. a•b = b•a for all $a$ and $b$ in G. However, some groups do have this property. These commutative groups are also called **Abelian** groups. The name comes from, not the Bible, but from Niels Henrik Abel who was a Norwegian mathematician. If $G$ has finitely many elements, we say that $G$ is a finite group. The **order of G** is the number of elements in G; it is denoted by $|G|$ or $\#G$. Next, let us examine several sets and operations commonly used in mathematics to see whether they form groups or not.

The first set is the set of integers (Z) and the operators are addition and multiplication. The algebraic properties of the combinations can be summarised as in the following table:

| | **Addition** | **Multiplication** |
|---|---|---|
| Closure | $a+b$ is an integer | $a*b$ is an integer |
| Associativity | $a+(b+c) = (a+b)+c$ | $a*(b*c) = (a*b)*c$ |
| Existence of an identity element | $a+0 = a$ | $a*1 = a$ |
| Existence of inverse elements | $a+(-a) = 0$ | Only 1 and -1 have inverses: 1*1 = 1, -1*(-1) = 1 |
| Commutativity | $a+b = b+a$ | $a*b = b*a$ |

From the table, we can conclude that (Z, +) is a group but (Z, *) is **not** a group. The reason why (Z, *) is not a group is that most of the elements do not have inverses. Furthermore, addition is commutative, so (Z, +) is an abelian group. The order of (Z, +) is infinite.

The next set is the set of remainders modulo a positive integer $n$ ($Z_n$), i.e. {0, 1, 2, ..., $n$-1}. The operations are addition modulo $n$ and addition modulo $n$.

| | **Addition modulo $n$** | **Multiplication modulo $n$** |
|---|---|---|
| Closure | $a+b \equiv c \bmod n$, $0 \leq c \leq n-1$ | $a*b \equiv c \bmod n$, $0 \leq c \leq n-1$ |
| Associativity | $a+(b+c) \equiv (a+b)+c \bmod n$ | $a*(b*c) \equiv (a*b)*c \bmod n$ |
| Existence of an identity element | $a+0 \equiv a \bmod n$ | $a*1 \equiv a \bmod n$ |
| Existence of inverse elements | $a+(n-a) \equiv 0 \bmod n$ | $a$ has the inverse only when $a$ is coprime to $n$ |
| Commutativity | $a+b \equiv b+a \bmod n$ | $a*b \equiv b*a \bmod n$ |

Again ($Z_n$, +) is a group and ($Z_n$, *) is not. ($Z_n$, +) is Abelian and finite. The order of ($Z_n$, +) is $n$. Note that 0 is an element of $Z_n$ and 0 is not coprime to any number so that is no inverse for 0. Therefore ($Z_n$, *) is not a group.

## Important

$Z_n$ (or Z/nZ) is usually used to denote the group ($Z_n$, +), i.e. the additive group of integers modulo n.

The last set is the set of remainders coprime to the modulus $n$. For example, when $n$ = 8, the set is {1, 3 , 5, 7}. In particular, when $n$ is a prime number, the set is {1, 2, ..., $n$-

1}. Let's call this set Coprime-n. The operators are are addition modulo *n* and addition modulo *n*.

| | **Addition modulo *n*** | **Multiplication modulo *n*** |
|---|---|---|
| Closure | *a+b* may be not in Coprime-n. | $a*b \equiv c$ mod *n*, *c* is in Coprime-n |
| Associativity | $a+(b+c) \equiv (a+b)+c \bmod n$ | $a*(b*c) \equiv (a*b)*c \bmod n$ |
| Existence of an identity element | *No* | $a*1 \equiv a \bmod n$ |
| Existence of inverse elements | *No* | the inverse exists for every *a* in Coprime-n |
| Commutativity | $a+b \equiv b+a \bmod n$ | $a*b \equiv b*a \bmod n$ |

Now (Coprime-n, +) is not a group and (Coprime-n, *) is a group. (Coprime-n, *) is Abelian and finite. When *n* is a prime number, the order of (Coprime-n, *) is *n-1*. **But this only holds when n is a prime number**. For example, when *n* =8, the order of (Coprime-8, *) is 4 not 7.

## Important

$Z_n^*$ is usually used to denote (Coprime-n, *), i.e. the multiplicative group of integers modulo n.

Now we are ready for finite fields. A field is a non-empty set *F* with **two** binary operators which are usually denoted by + and *, that satisfy the usual arithmetic properties:

- (*F*, +) is an Abelian group with (additive) identity denoted by 0.
- ($F\backslash\{0\}$, ·) is an Abelian group with (multiplicative) identity denoted by 1.
- The distributive law holds: (a+b)*c = a*c+b*c for all a, b, c ∈ *F*.

If the set *F* is finite, then the field is said to be a **finite field**. The **order** of a finite field is the number of elements in the finite field. By definition, (*Z*, +, *) does not form a field because ($Z\backslash\{0\}$, *) is not a multiplicative group. ($Z_n$, +, *) in general is not a finite field. For example, $Z_8/\{0\}$ = {1, 2, 3, 4, 5, 6, 7} along with modulo 8 multiplication does not form a group. However, when *n* is a prime number, things become different. For example $Z_5/\{0\}$ ={1, 2, 3, 4} along with modulo 5 multiplication forms the Abelian group $Z_5^*$. Therefore, ($Z_5$, +, *) is a finite field. There is a (not so funny) limerick may help you memorise this fact:

> In arctic and tropical climes,
>
> The integers, addition, and times,

Taken (mod $p$) will yield

A full finite field,

As $p$ ranges over the primes.

---

Prev
Chapter 3. Modular Arithmetic

Home

Next
Galois' Theorem and Polynomial Arithmetic