

**Definition:** Let  $\mathbb{F}$  be a (non-empty) set with two operations (addition and multiplication).

Suppose that:

- $\mathbb{F}$  is an abelian group under addition.
- For all  $a, b, c \in \mathbb{F}$  we have that  $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$ .
- $\mathbb{F}$  is a monoid under multiplication (i.e. for all  $a, b, c \in \mathbb{F}$ ,  $(ab)c = a(bc)$  and there exists some element  $1 \in \mathbb{F}$ , such that  $a1 = 1a = a$  for all  $a \in \mathbb{F}$ ) such that  $1 \neq 0$ .

Then  $\mathbb{F}$  is a **ring**. If in addition:

- Multiplication is commutative (i.e.  $ab = ba$  for all  $a, b \in \mathbb{F}$ ).
- For all  $a \in \mathbb{F}^\times = \{x \in \mathbb{F} \mid x \neq 0\}$ ,  $a^{-1} \in \mathbb{F}^\times$  exists where  $aa^{-1} = a^{-1}a = 1$  (i.e. all non-zero elements are units).

Then  $\mathbb{F}$  is a **field**.

Let  $\mathbb{F}$  be a field. Consider  $1 + 1 + \cdots + 1 = n1$ . Let  $n \in \mathbb{Z}$  be the smallest positive integer such that  $n1 = 0$ . In this case, we say the **characteristic** of  $\mathbb{F}$  is  $n$ . If no such  $n$  exists, we say that  $\mathbb{F}$  has **characteristic** 0.

**Examples:**  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  (the rational, real, and complex numbers) are all fields of characteristic 0. Notice that  $\mathbb{Q}$  is the subfield generated by the multiplicative identity 1 in each of these cases. In fact, one can show that  $\mathbb{Q}$  is the “smallest” field of characteristic 0 and there is an isomorphic copy of  $\mathbb{Q}$  contained in any field of characteristic 0.

**Finite Examples:**  $\mathbb{Z}_p$  where  $p$  a prime is a field of characteristic  $p$ .

**Theorem:** Let  $\mathbb{F}$  be a (finite) field of order  $q$ . Then  $q = p^k$  for some prime  $p$  and positive integer  $k$ . Also,  $\mathbb{F}$  has characteristic  $p$  and the subfield generated by 1 is isomorphic to  $\mathbb{Z}_p$ . Moreover, for each prime  $p$  and positive integer  $k$  there exists a (finite) field  $\mathbb{F}_q$  of order  $q = p^k$ .  $\mathbb{F}_q$  is the unique field of order  $q$  (up to isomorphism). Also,  $\mathbb{F}_q^\times$  (the non-zero elements) forms a *cyclic* group under multiplication.

**A Field with Nine Elements:** Consider  $\mathbb{F}_9 = \mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$  where  $i^2 = -1$  ( $= 2 \pmod{3}$ ).  $\mathbb{F}_9$  is the field of order 9.

**Addition:**  $(a + bi) + (c + di) = (a + c) + (b + d)i$  where  $a + c$  and  $b + d$  are computed in  $\mathbb{Z}_3$ .

**Multiplication:**  $(a + bi)(c + di) = (ac + bdi^2) + (ad + bc)i = (ac + 2bd) + (ad + bc)i$  where  $ac + 2bd$  and  $ad + bc$  are computed in  $\mathbb{Z}_3$ .

The addition and multiplication tables for this field are on the next page (notice the copy of  $\mathbb{Z}_3$  living inside  $\mathbb{F}_9$ ).

**A Field with Eight Elements:** Consider  $\mathbb{F}_8 = \mathbb{Z}_2[\alpha] = \{a\alpha^2 + b\alpha + c \mid a, b, c \in \mathbb{Z}_2\}$  where  $\alpha^3 = \alpha + 1$ .  $\mathbb{F}_8$  is the field of order 8.

**Addition:**  $(a\alpha^2 + b\alpha + c) + (x\alpha^2 + y\alpha + z) = (a + x)\alpha^2 + (b + y)\alpha + (c + z)$  where  $a + x$ ,  $b + y$ , and  $c + z$  are computed in  $\mathbb{Z}_2$ .

**Multiplication:**  $(a\alpha^2 + b\alpha + c)(x\alpha^2 + y\alpha + z) = ax\alpha^4 + (ay + bx)\alpha^3 + (az + by + cx)\alpha^2 + (bz + cy)\alpha + cz = ax\alpha(\alpha + 1) + (ay + bx)(\alpha + 1) + (az + by + cx)\alpha^2 + (bz + cy)\alpha + cz = \dots$  where coefficients of  $\alpha$  are computed in  $\mathbb{Z}_2$ .

The Addition Table for  $\mathbb{F}_9$ :

+	0	1	2	$i$	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
0	0	1	2	$i$	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
1	1	2	0	$1+i$	$2+i$	$i$	$1+2i$	$2+2i$	$2i$
2	2	0	1	$2+i$	$i$	$1+i$	$2+2i$	$2i$	$1+2i$
$i$	$i$	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$	0	1	2
$1+i$	$1+i$	$2+i$	$i$	$1+2i$	$2+2i$	$2i$	1	2	0
$2+i$	$2+i$	$i$	$1+i$	$2+2i$	$2i$	$1+2i$	2	0	1
$2i$	$2i$	$1+2i$	$2+2i$	0	1	2	$i$	$1+i$	$2+i$
$1+2i$	$1+2i$	$2+2i$	$2i$	1	2	0	$1+i$	$2+i$	$i$
$2+2i$	$2+2i$	$2i$	$1+2i$	2	0	1	$2+i$	$i$	$1+i$

The Multiplication Table for  $\mathbb{F}_9$ :

$\times$	0	1	2	$i$	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$i$	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
2	0	2	1	$2i$	$2+2i$	$1+2i$	$i$	$2+i$	$1+i$
$i$	0	$i$	$2i$	2	$2+i$	$2+2i$	1	$1+i$	$1+2i$
$1+i$	0	$1+i$	$2+2i$	$2+i$	$2i$	1	$1+2i$	2	$i$
$2+i$	0	$2+i$	$1+2i$	$2+2i$	1	$i$	$1+i$	$2i$	2
$2i$	0	$2i$	$i$	1	$1+2i$	$1+i$	2	$2+2i$	$2+i$
$1+2i$	0	$1+2i$	$2+i$	$1+i$	2	$2i$	$2+2i$	$i$	1
$2+2i$	0	$2+2i$	$1+i$	$1+2i$	$i$	2	$2+i$	1	$2i$

**Note:**  $1+i$  generates the multiplicative group  $\mathbb{F}_9^\times$ .