

# Mathematics 201: Fields

## Fields defined

Informally, a *field* is a mathematical system in which the usual rules of arithmetic are valid.

More precisely, the concept *field* is expressed in the following definition, which should be memorized.

**Definition 1.1 (Field).** A field is a set  $k$  with two operations,  $(a, b) \mapsto a + b$  (“addition”) and  $(a, b) \mapsto a \cdot b$  (“multiplication”), and distinguished elements  $0$  and  $1$  with  $0 \neq 1$ , so that the following are true:

	Addition	Multiplication
<i>Associative:</i>	$(\forall a, b, c \in k)$ $(a + b) + c = a + (b + c)$	$(\forall a, b, c \in k)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
<i>Commutative:</i>	$(\forall a, b \in k)$ $a + b = b + a$	$(\forall a, b \in k)$ $a \cdot b = b \cdot a$
<i>Identities 0, 1:</i>	$(\forall a \in k)(a + 0 = a)$	$(\forall a \in k)(1 \cdot a = a)$
<i>Inverses:</i>	$(\forall a \in k)$ $(\exists z \in k)(a + z = 0)$	$(\forall a \in k)$ $(a \neq 0 \rightarrow (\exists z \in k)(a \cdot z = 1))$
<i>Distributive Law</i>	$(\forall a, b, c \in k)$ $a \cdot (b + c) = a \cdot b + a \cdot c$	

The additive inverse of  $a$  is called the *negative* of  $a$ , and is written  $-a$ . *Subtraction* is defined by  $a - b = a + (-b)$ .

The multiplicative inverse of  $a \neq 0$  is called the *reciprocal* of  $a$ , and is written  $a^{-1}$ . *Division* is defined by  $a/b = a \cdot b^{-1}$  provided  $b \neq 0$ . When convenient we write  $ab$  for  $a \cdot b$ .

The rational number system  $\mathbf{Q}$ , the real number system  $\mathbf{R}$  and the complex number system  $\mathbf{C}$  are fields. For any prime  $p$ , the set  $\{0, 1, \dots, p - 1\}$  with the operations of addition and subtraction mod  $p$  forms a *finite field* called  $\mathbf{F}_p$ .

## The Field $\mathbf{F}_7$

The *elements* of the field  $\mathbf{F}_7$  are  $\{0, 1, 2, 3, 4, 5, 6\}$ . The sum  $a+b$  and product  $a \cdot b$  in  $\mathbf{F}_7$  are defined by taking the ordinary sum and product and replacing them by their remainders when divided by 7. Thus, in  $\mathbf{F}_7$ ,

$$5 + 4 = 2$$

because  $5 + 4 = 9 = 1 \cdot 7 + 2$ . Likewise,

$$5 \cdot 4 = 6$$

in  $\mathbf{F}_7$  because  $5 \cdot 4 = 20 = 2 \cdot 7 + 6$ .

We call these operations “addition and multiplication mod seven”; they work because of the following theorem from arithmetic.

**Theorem 1.1 (Division Algorithm).** *For any integer  $m$  (the “dividend”) and natural number  $n$  (the “divisor”), there exist unique integers  $q$  (the “quotient”) and  $r$  (the “remainder”) with  $0 \leq r < n$  such that*

$$m = n \cdot q + r.$$

### Exercises

- (a) Verify that  $0 \in \mathbf{F}_7$  is the identity for addition in  $\mathbf{F}_7$  and  $1 \in \mathbf{F}_7$  is the identity for multiplication in  $\mathbf{F}_7$ .
- (b) According to the definition of field, to every  $a \in \mathbf{F}_7$  there corresponds an element  $-a$  such that  $a + (-a) = 0$ . Find  $-a$  for each  $a \in \{0, 1, 2, 3, 4, 5, 6\}$ .
- (c) For each  $a \in \{0, 1, 2, 3, 4, 5, 6\}$  calculate the product  $6 \cdot a$  in  $\mathbf{F}_7$  and compare the result to  $-a$  that you found in part (b).
- (d) According to the definition of field, to every nonzero  $a \in \mathbf{F}_7$  there corresponds an element  $a^{-1}$  such that  $a \cdot a^{-1} = 1$ . Find  $a^{-1}$  for each  $a \in \{1, 2, 3, 4, 5, 6\}$ . (It may help to construct the entire multiplication table.)