EXAMPLE 6.10

The set of positive real numbers $\mathbb{R}^+$ with the operation of multiplication is also an Abelian group. This time, the identity is 1 and the inverse of $r \in \mathbb{R}^+$ is $1/r$. □

EXAMPLE 6.11

The set of $n \times n$ real matrices with the operation of matrix addition is a group. The zero matrix is the identity and the inverse of a matrix M is the matrix $-M$, consisting of the same elements as M but with their signs reversed. □

EXAMPLE 6.12

The set of non-singular $n \times n$ real matrices with the operation of matrix multiplication is a group for any positive integer n. The identity matrix is the group identity and the inverse of a matrix is its group inverse. These groups are not commutative. □

Groups are not used directly in the construction of error-correcting codes. They form the basis for more complex algebraic structures which are used.

6.3 Rings and Fields

Having two operations that interact with each other makes things more interesting.

DEFINITION 6.6 Ring *A* ring *is a triple $(R, +, \times)$ consisting of a set R, and two operations $+$ and $\times$, referred to as* addition *and* multiplication*, respectively, which satisfy the following conditions:*

1. associativity of $+$: $a + (b + c) = (a + b) + c$ *for all* $a, b, c \in R$*;*
2. commutativity of $+$: $a + b = b + a$ *for all* $a, b \in R$*;*
3. existence of additive identity: *there exists* $0 \in R$ *such that* $0 + a = a$ *and* $a + 0 = a$ *for all* $a \in R$*;*
4. existence of additive inverses: *for each* $a \in R$ *there exists* $-a \in R$ *such that* $a + (-a) = 0$ *and* $(-a) + a = 0$*;*
5. associativity of $\times$: $a \times (b \times c) = (a \times b) \times c$ *for all* $a, b, c \in R$*;*
6. distributivity of $\times$ over $+$: $a \times (b + c) = (a \times b) + (a \times c)$ *for all* $a, b, c \in R$.