Fields

Vahid Meghdadi

February 2008

A field $< \mathbf{F}, +, . >$ is a set of objects $\mathbf{F}$ on which the operation of addition and multiplication apply in a manner analogous to the way these operations work for real numbers. In addition the following conditions are satisfied:

1. Closure under addition: if a and $b \in \mathbf{F}$ then $a + b \in \mathbf{F}$.
2. Additive identity: there is an element in $\mathbf{F}$, which is denoted by 0, such that $0 + a = a$ for every a in $\mathbf{F}$.
3. Additive inverse: for every $a \in \mathbf{F}$ there is an element $b \in \mathbf{F}$ such that $a + b = b + a = 0$. This element is denoted as $-a$.
4. Associativity: $(a + b) + c = a + (b + c)$ for every $a, b, c \in \mathbf{F}$.
5. Commutativity: $a + b = b + a$ for every $a, b \in \mathbf{F}$.
6. Closure under multiplication: For every $a, b \in \mathbf{F}, a.b$ is also in $\mathbf{F}$.
7. Multiplicative identity: There is an element in $\mathbf{F}$, which is denoted by 1, such that $1.a = a.1 = a$
8. Multiplicative inverse: For every $a \in \mathbf{F}$ with $a \neq 0$, there is an element $b \in \mathbf{F}$ such that $a.b = b.a = 1$. This element is called the inverse of a an denoted by a^{-1}.
9. Associativity: $(a.b).c = a.(b.c)$ for every $a, b, c \in \mathbf{F}$.
10. Commutativity: $a.b = b.a$ for every $a, b \in \mathbf{F}$.
11. Multiplication distributes over addition: $a.(b + c) = a.b + a.c$.

The field $< \mathbf{F}, +, . >$ with q elements in it may be denoted by $\mathbf{F}_q$.