Fields

August 23, 2000

**Definition 1** A field, $\mathcal{F}$, is a quintuple $(F, +, \cdot, 0, 1)$ where $F$ is a nonempty set (called the underlying set of $\mathcal{F}$), $+$ is a binary operation on $F$ called addition, $\cdot$ is a binary operation on $F$ called multiplication, $0$ is an element of $F$ called the additive identity (or zero) of $\mathcal{F}$, and $1$ is an element of $F$ (with $1 \neq 0$) called the multiplicative identity (or one) of $\mathcal{F}$ such that the following properties hold:

**Commutative Properties** For all $x$ and $y \in F$, $x + y = y + x$ and $x \cdot y = y \cdot x$.

**Associative Properties** For all $x$, $y$, and $z \in F$, $x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

**Identity Properties** For all $x \in F$, $x + 0 = x$ and $x \cdot 1 = x$.

**Inverse Properties** For all $x \in F$, there exists $-x \in F$ such that $x + (-x) = 0$, and for all $x \in F$ with $x \neq 0$, there exists $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$.

**Distributive Property** For all $x$, $y$, and $z \in F$, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

**Remark 2** Usually, once the operations $(+, \cdot)$ and the additive and multiplicative identities $(0, 1)$ of a field have been defined, we just refer to the field as $F$. Strictly speaking, the field is really $\mathcal{F} = (F, +, \cdot, 0, 1)$ but we save a lot of space by just saying “the field $F$”.

**Remark 3** The operation of multiplication, $\cdot$, is sometimes described simply by juxtaposition of the elements of $F$ being multiplied. That is, instead of writing $x \cdot y$, we just write $xy$. 

1
Example 4 The field \( Z_3 \) is the field whose underlying set has three elements \( \{0, 1, 2\} \) where the symbols 0, 1, 2 should not be thought of as the usual integers because addition and multiplication in \( Z_3 \) are defined as given in the following tables

\[
\begin{array}{c|cc}
+ & 0 & 1 & 2 \\
\hline
0 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
2 & 2 & 0 & 1 \\
\end{array}
\quad
\begin{array}{c|ccc}
\cdot & 0 & 1 & 2 \\
\hline
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 \\
2 & 0 & 2 & 1 \\
\end{array}
\]

Note that addition and multiplication in \( Z_3 \) have been defined such that

\[ x + y = \text{the remainder when “the usual } x + y \text{” is divided by 3} \]

and

\[ x \cdot y = \text{the remainder when “the usual } x \cdot y \text{” is divided by 3}. \]

For example, if we do “the usual” addition 1 + 2, we get the answer 3 and

\[ \frac{3}{3} = 1 \text{ remainder 0} \]

so, in \( Z_3 \), we define \( 1 + 2 = 0 \).

Likewise, if we do “the usual” multiplication \( 1 \cdot 2 \), we get the answer 2 and

\[ \frac{2}{3} = 0 \text{ remainder 2} \]

so, in \( Z_3 \), we define \( 1 \cdot 2 = 2 \).

Exercise 5 Prove that \( Z_3 \) is a field. What are the additive and multiplicative identities of \( Z_3 \)? For each \( x \in Z_3 \), what is \(-x\) and, for each non-zero \( x \), what is \( x^{-1} \)?

Exercise 6 Mimic the construction of \( Z_3 \) to construct the set \( Z_4 \) which has four elements \( \{0, 1, 2, 3\} \). Make addition and multiplication tables for \( Z_4 \). Is \( Z_4 \) a field? What about \( Z_5 \)?

The following theorem establishes that we can “cancel” when doing addition or multiplication in a field.
Theorem 7 (Cancellation Properties) If $F$ is a field, $x$, $y$, and $z \in F$, and $x + z = y + z$, then $x = y$. Also, if $z \neq 0$ and $x \cdot z = y \cdot z$, then $x = y$.

Proof. Supposing that $x + z = y + z$, we obtain

$$(x + z) + (-z) = (y + z) + (-z).$$

Using the associative property of addition, we then obtain

$$x + (z + (-z)) = y + (z + (-z)).$$

Using the fact that $z + (-z) = 0$ (the additive inverse property), we obtain

$$x + 0 = y + 0.$$  

We now use the fact that $x + 0 = x$ and $y + 0 = y$ (additive identity property) to conclude that $x = y$.

We leave the proof of the multiplicative cancellation property as homework. ■

A very useful fact that follows from the additive cancellation property and the field axioms is given in the following theorem.

Theorem 8 If $F$ is a field and $x \in F$, then $x \cdot 0 = 0$.

Proof. Let $x \in F$ be given. Our line of reasoning is as follows:

$$0 + 0 = 0 \quad \text{(additive identity property)}$$
$$\implies x \cdot (0 + 0) = x \cdot 0 \quad \text{(multiplication by $x$)}$$
$$\implies (x \cdot 0) + (x \cdot 0) = x \cdot 0 \quad \text{(distributive property)}$$

but we also know that $(x \cdot 0) + 0 = (x \cdot 0)$ by the additive identity property so we conclude that

$$(x \cdot 0) + (x \cdot 0) = (x \cdot 0) + 0$$

or, by the commutative property of addition,

$$(x \cdot 0) + (x \cdot 0) = 0 + (x \cdot 0).$$

Finally, we apply the cancellation law of addition (Theorem 7) to obtain $x \cdot 0 = 0$. ■
Exercise 9 Prove that if $F$ is a field, $x$ and $y \in F$, and $x + y = x$, then $y = 0$.

Exercise 10 Prove that if $F$ is a field, $x$ and $y \in F$ with $x \neq 0$, and $xy = x$, then $y = 1$.

Exercise 11 Prove that if $F$ is a field, then the additive inverse of any element $x \in F$ is unique. In other words, prove that if $F$ is a field, $x \in F$, $y \in F$, and $x + y = 0$, then $y = -x$.

Exercise 12 Prove that if $F$ is a field, then the multiplicative inverse of any non-zero element $x \in F$ is unique. In other words, prove that if $F$ is a field, $x \in F$ with $x \neq 0$, $y \in F$, and $x \cdot y = 1$, then $y = x^{-1}$.

Exercise 13 Use the results of the previous two exercises to prove that if $F$ is a field, then $-0 = 0$ and $1^{-1} = 1$.

In what follows, we let $R$ denote the set of all real numbers with addition and multiplication defined in the usual way (the way you always learned!). For example, $4 + 5 = 9$, $(-3) \cdot 6 = -18$, $(4/5) + (1/3) = 17/15$, $(2 + \sqrt{2}) \cdot (3 - 4\sqrt{3}) = 6 - 8\sqrt{3} + 3\sqrt{2} - 4\sqrt{6}$, etc. In this case, we know (from previous experience) that the commutative, associative, and distributive properties hold and it is easy to see that $R$ is a field.

For the remainder, we take $R$ to be the “universal field” and we define the subsets, $N$, $Z$, and $Q$, of $R$ as follows:

$N =$ the set of all natural numbers $= \{1, 2, 3, \ldots \}$

$Z =$ the set of all integers $= \{0, 1, -1, 2, -2, 3, \ldots \}$

$Q =$ the set of rational numbers $= \left\{ \frac{a}{b} \mid a \in Z, \ b \in Z, \text{ and } b \neq 0 \right\}$

Clearly, $N \subseteq Z \subseteq Q \subseteq R$.

Exercise 14 Explain why $N$ is not a field and explain why $Z$ is not a field.

Exercise 15 Prove that $Q$ is a field.

Exercise 16 Prove that if $F$ is a field with $F \subseteq R$ (in other words, if $F$ is a subfield of $R$), then $Q \subseteq F$. This establishes the fact that $Q$ is the “smallest” subfield of $R$. 

4
Does $R$ have any proper subfields that are bigger than $Q$? The answer is yes!

**Exercise 17** Define

$$F_{\sqrt{2}} = \left\{ p + q\sqrt{2} \mid p \in Q, q \in Q \right\}.$$  

Prove that $F$ is a field and that $Q \subset F_{\sqrt{2}} \subset R$. 