

Mathematics 201: Fields, First Proofs

In elementary algebra we learned that if $a + b = a + c$ then $b = c$; this is called the *cancellation property* for addition,

Theorem 12.1 (Cancellation property of addition). *Let k be a field, and let $a, b, c \in k$. If $a + b = a + c$, then $b = c$.*

Proof. Let k be a field, let $a, b, c \in k$, and assume

$$a + b = a + c. \tag{1}$$

By the definition of field, a has an additive inverse, $-a$. Adding $-a$ to both sides of Equation (1) and using basic properties of fields to simplify gives

$$\begin{aligned} -a + (a + b) &= -a + (a + c), \\ (-a + a) + b &= (-a + a) + c, && \text{(Associative Law)} \\ 0 + b &= 0 + c, && \text{(Additive Inverse)} \\ b &= c, && \text{(Identity 0)} \end{aligned}$$

We have shown that if $a + b = a + c$ then $b = c$, so the proof is complete. \square

Corollary. *In a field k , every element a has exactly one additive inverse.*

Proof. Let k be a field, $a \in k$. There exists an element $-a \in k$ such that $a + (-a) = 0$. Let x be any element of k such that $a + x = 0$. Then $a + x = a + (-a)$, and it follows from Theorem 12.1 that $x = -a$. \square

Assignment: State and prove an analogue for multiplication of Theorem 12.1 and its Corollary.

We conclude with two simple facts about fields. First in any field, multiplying any element by zero gives zero.

Theorem 12.2. *Let k be a field. For all $a \in k$, $a \cdot 0 = 0$.*

Proof. Let k be a field, and let $a \in k$ be arbitrary. We show that $a \cdot 0 = 0$ by a direct proof. Calculate

$$\begin{aligned} a \cdot 0 + a \cdot 0 &= a \cdot (0 + 0) && \text{(Distributive Law)} \\ &= a \cdot 0 && \text{(Identity 0),} \end{aligned}$$

thus

$$a \cdot 0 + a \cdot 0 = a \cdot 0.$$

Subtracting $a \cdot 0$ from both sides and simplifying gives $a \cdot 0 = 0$. We have shown for arbitrary $a \in k$ that $a \cdot 0 = 0$, so the proof is complete. \square

Finally, here is a property that the element -1 has in any field.

Theorem 12.3. *Let k be a field, and $a \in k$ be arbitrary. Then $(-1) \cdot a = -a$.*

Proof. By the Corollary to Theorem 12.1, it suffices to show that $a + (-1) \cdot a = 0$. So calculate

$$\begin{aligned} a + (-1) \cdot a &= 1 \cdot a + (-1) \cdot a && \text{(Identity 1)} \\ &= (1 + (-1)) \cdot a && \text{(Distributive Law)} \\ &= 0 \cdot a && \text{(Additive inverse)} \\ &= 0 \end{aligned}$$

by the Theorem just proven. We have shown that $(-1) \cdot a$ is the additive inverse of a , so the proof is complete. \square