Lemma. *Cancellation Property*

$$\forall a, b, c \in \mathbb{F} : a + c = b + c \Leftrightarrow a = b \tag{1}$$
$$\forall a, b, c \in \mathbb{F}, c \neq 0 : ac = bc \Leftrightarrow a = b \tag{2}$$

Proof. Suppose $a + c = b + c$.

$\exists\ (-c) : c + (-c) = 0$	Existence of an Additive Inverse	(3)
$\Rightarrow\ (a + c) + (-c) = (b + c) + (-c)$	Definition of $=$	(4)
$\Rightarrow\ a + (c + (-c)) = b + (c + (-c))$	Associative Law	(5)
$\Rightarrow\ a + 0 = b + 0$	Existence of an Additive Inverse	(6)
$\Rightarrow\ a = b$	Existence of an Additive Identity	(7)

Suppose now $ac = bc$.

$\exists\ c^{-1} : cc^{-1} = 1$	Existence of an Additive Inverse	(8)
$\Rightarrow\ (ac)c^{-1} = (bc)c^{-1}$	Definition of $=$	(9)
$\Rightarrow\ a(cc^{-1}) = b(cc^{-1})$	Associative Law	(10)
$\Rightarrow\ a \cdot 1 = b \cdot 1$	Existence of a Multiplicative Inverse	(11)
$\Rightarrow\ a = b$	Existence of an Additive Identity	(12)

□

Lemma 0.1. $\forall a, b \in \mathbb{F} : (-a)b = -ab$

Proof.

$ab + (-a)b = ba + b(-a)$	Commutative Law	(1)
$a + (-a) = 0$	Existence of an Additive Inverse	(2)
$\Rightarrow b(a + (-a)) = b \cdot 0$	Distributive Law	(3)
	and Existence of an Additive Inverse	(4)
$= 0$	Lemma 0.2	(5)
$\Rightarrow ab + (-a)b = 0$	Definition of $=$	(6)
$\Rightarrow (-a)b + ab = 0$	Commutative Law	(7)
$(-a)b + ab - ab = 0 - ab$	Definition of $=$	(8)
$\Rightarrow (-a)b + 0 = -ab$	Existence of an Additive Inverse	(9)
	and Existence of an Additive Identity	
$= (-a)b$	Existence of an Additive Identity	(10)

□

Corollary 0.1.1. $\forall a \in \mathbb{F} : -b = (-1)b$

Proof. From Lemma 0.1, if $a = 1$, then $(-1)b = -1 \cdot b$

$-1 \cdot b = -b \cdot 1$	Commutative Law	(1)
$\Rightarrow (-1)b = -b$	Definition of $=$	(2)
	and Existence of a Multiplicative Identity	

□

Lemma 0.2. $\forall a \in \mathbb{F} : a \cdot 0 = 0$

Proof.

$$\begin{aligned}
0 + 0 &= 0 && \text{Existence of an Additive Identity} && (1)\\
\Rightarrow a \cdot (0+0) &= a \cdot 0 + a \cdot 0 && \text{Distributive Law} && (2)\\
&= a \cdot 0 && \text{Definition of} = && (3)\\
(a \cdot 0 + a \cdot 0) - (a \cdot 0) &= a \cdot 0 - (a \cdot 0) && \text{Definition of} = && (4)\\
\Rightarrow a \cdot 0 + (a \cdot 0 - a \cdot 0) &= 0 && \text{Associative Law} && (5)\\
& && \text{and Existence of an Additive Inverse} && \\
\Rightarrow a \cdot 0 + 0 &= 0 && \text{Existence of an Additive Inverse} && (6)\\
\Rightarrow a \cdot 0 &= 0 && \text{Existence of an Additive Identity} &&
\end{aligned}$$

□

Lemma 0.3. $-(-a) = a$

Proof.

$$\begin{aligned}
a + (-a) &= 0 && \text{Existence of an Additive Inverse} && (1)\\
(-1)(a + (-a)) &= (-1)0 && \text{Definition of} = && (2)\\
(-1)a + (-1)(-a) &= 0 && \text{Distributive Law} && (3)\\
& && \text{and Lemma 0.2} && \\
\Leftrightarrow -a - (-a) &= 0 && \text{Corollary 0.1.1} && (4)\\
a + (-a - (-a)) &= a + 0 && \text{Definition of} = && (5)\\
(a - a) - (-a) &= a && \text{Associative Law} && (6)\\
& && \text{and Existence of an Additive Identity} && (7)\\
0 - (-a) &= a && \text{Existence of an Additive Inverse} && (8)\\
-(-a) &= a && \text{Existence of an Additive Identity} && (9)
\end{aligned}$$

□

Lemma 0.4. $\forall a, b \in \mathbb{F} : ab = 0 \Leftrightarrow a = 0 \vee b = 0$

Proof. By Commutative Law and Lemma 0.2, $a = 0 \Rightarrow ab = ba = b \cdot 0 = 0$.

Similarly, $b = 0 \Rightarrow ab = a \cdot 0 = 0$. If $ab = 0$ and $b \neq 0$, $\exists\ b^{-1} : abb^{-1} = 0 \cdot b^{-1}$, hence by Commutative Law and Existence of a Multiplicative Inverse $a \cdot 1 = b^{-1} \cdot 0$, then by Existence of a Multiplicative Identity and Lemma 0.2 $a = 0$.

If $ab = 0$ and $a \neq 0$, $\exists\ a^{-1} : a^{-1}ab = a^{-1} \cdot 0$, hence by Commutative Law and Lemma 0.2 $aa^{-1}b = 0$, then by Existence of a Multiplicative Inverse $1 \cdot b = 0$, and by Commutative Law and Existence of a Multiplicative Identity $b \cdot 1 = b = 0$.

If $a = 0 \wedge b = 0$, then by Lemma 0.2 $ab = 0 \cdot 0 = 0$ □

Theorem. *Let $\mathbb{F}$ be a field with 3 elements $0, 1, a$. Then the following is true:*

1. $1 + 1 = a$

2. $a + 1 = 0$

3. $a \cdot a = 1$

Proof. Consider $a \cdot a$. By Multiplicative Closure of $\mathbb{F}$, there are three cases:

1. $a \cdot a = a$

2. $a \cdot a = 0$

3. $a \cdot a = 1$

We argue by repetitive *reductio ad absurdum* that $a \cdot a = 1$.

Suppose that $a \cdot a = a$. By distinctness of elements, $a \neq 0$. Therefore by Cancellation Property $a = 1$, which contradicts the distinctness of elements.

Suppose now that $a \cdot a = 0$. Since $a = a$ and Lemma 0.4, $a = 0$, which again contradicts the distinctness of elements.

Hence, $a \cdot a = 1$.

Therefore, $a + a \cdot a = a + 1$. From Distributive Law, $a(a+1) = (a+1)$. By Cancellation Property , $a(a+1) - (a+1) = 0$. By Commutative Law and Distributive Law, $(a+1)(a-1)$=0. From Lemma 0.4, Cancellation Property and distinctness of elements, $a = -1 \ \veebar \ a = 1$. Since $a \neq 1$ by definition, $a = -1$.

Therefore, $a + 1 = -1 + 1 = 1 + (-1)$[by Commutative Law] $= 0$ [by Existence of an Additive Inverse].

We now prove that $1 + 1 = 0$.

Suppose on the contrary that $1 + 1 = 1$.

Then by cancellation property $1 = 0$, which is a contradiction to Distinctness of an Additive Identity and Multiplicative Identity $\Rightarrow (1 + 1 = 0) \vee (1 + 1 = a)$.

If $1 + 1 = 0$, then $(1 + 1) + a = 0 + a = a$ by Existence of an Additive Identity . But then by Associative Law , Commutative Law and Existence of an Additive Identity $1 + (1 + a) = 1 + (a + 1) = 1 + 0 = 1$ and hence $1 = a$, which is a contradiction, since a and 1 are distinct by definition. Therefore, $1 + 1 = a = -1$. $\square$