APPENDIX

Supporting Proofs

Claim. The triple $(\{ a, b \}, +, \cdot)$ with operations defined as below, constitutes a field.

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

Proof. First, it is to be shown $(\{ a, b \}, +)$ is an Abelian group. From the table above at left, it is clear $+$ is well-defined on $\{ a, b \}$. Moreover, a serves as additive identity, and each element is its own additive inverse. As a and b are the only elements in the set, commutativity follows from the fact that $a + b = b + a$. To be thorough, it must be verified $+$ is associative. This is illustrated with the following cases:

$$
\begin{array}{llclcllcl}
\text{(i)} & a + (a + a) & = & a + a & = & (a + a) + a & & & ; \\
\text{(ii)} & a + (b + a) & = & a + b & = & b + a & = & (a + b) + a & ; \\
\text{(iii)} & b + (a + b) & = & b + b & = & (b + a) + b & & & ; \\
\text{(iv)} & b + (b + b) & = & b + a & = & a + b & = & (b + b) + b & .
\end{array}
$$

Now, the set $\{ a, b \}$ is clearly closed under $\cdot$, and it must be shown the nonzero elements (where zero element refers to additive identity, a in this case) form an Abelian group under $\cdot$ as well. Fortunately, the only nonzero element is b, and the set $\{ b \}$ under $\cdot$ is trivially Abelian due to possessing a singular possible product.

Finally, it must be shown the distributive law of $+$ over $\cdot$ holds. Happily, all cases can be presented thus (where $a \cdot b$ is written ab):

$$
\begin{array}{llclclclcll}
\text{(i)} & (a + a) \cdot a & = & aa & = & a & = & a + a & = & (aa) + (aa) & ; \\
\text{(ii)} & (a + b) \cdot a & = & ba & = & a & = & a + a & = & (aa) + (ba) & ; \\
\text{(iii)} & (b + b) \cdot a & = & aa & = & a & = & a + a & = & (ba) + (ba) & ; \\
\text{(iv)} & (a + a) \cdot b & = & ab & = & a & = & a + a & = & (ab) + (ab) & ; \\
\text{(v)} & (a + b) \cdot b & = & bb & = & b & = & a + b & = & (ab) + (bb) & ; \\
\text{(vi)} & (b + b) \cdot b & = & ab & = & a & = & b + b & = & (bb) + (bb) & .
\end{array}
$$

This completes the proof.

Claim. The fields[1] $(\{\,e, o\,\}, +, \cdot\,)$ and $(\{\,0, 1\,\}, +_2, \cdot\,)$ with operations defined as below, are isomorphic.

$+$	e	o
e	e	o
o	o	e

$\cdot$	e	o
e	e	e
o	e	o

$+_2$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Proof. Define a function $f: \{\,e, o\,\} \longrightarrow \{\,0, 1\,\}$ by $f(e) = 0$ and $f(o) = 1$. This way, it is clear f is a one to one correspondence. Therefore, if it can be shown that for each choice of x and y in $\{\,e, o\,\}$ the ***homomorphism property*** holds:

$$f(x+y) = f(x) +_2 f(y)\,;$$

$$f(xy) = f(x)f(y),$$

then it follows f is an isomorphism of fields. All possible cases are shown below.

$$\begin{array}{llllllllll}
\text{(i)} & f(e+e) & = & f(e) & = & 0 & = & 0 +_2 0 & = & f(e) +_2 f(e)\;; \\
\text{(ii)} & f(e+o) & = & f(o) & = & 1 & = & 0 +_2 1 & = & f(e) +_2 f(o)\;; \\
\text{(iii)} & f(o+o) & = & f(e) & = & 0 & = & 1 +_2 1 & = & f(o) +_2 f(o)\;; \\
 & & & & & & & & & \\
\text{(iv)} & f(ee) & = & f(e) & = & 0 & = & (0)(0) & = & f(e)f(e)\;; \\
\text{(v)} & f(eo) & = & f(e) & = & 0 & = & (0)(1) & = & f(e)f(o)\;; \\
\text{(vi)} & f(oo) & = & f(o) & = & 1 & = & (1)(1) & = & f(o)f(o)\;.
\end{array}$$

Conclude $(\{\,e, o\,\}, +, \cdot\,)$ and $(\{\,0, 1\,\}, +_2, \cdot\,)$ are indeed isomorphic.

[1] The proof may be undertaken similarly for any of the examples of GF(2) in this post.