Ex. #5 of a field.

$F_7 = \{0,1,2,3,4,5,6\}$ → [2 through 6 could have been named anything else.]

+	0	1	2	3	4	5	6
0							
1		2					
2							
3							
4	4	5	6	0	1	2	3
5					2		
6							

Rule: Remainders when you divide by 7. (remainders mod 7)

$2 \times 2 = 4 \to$ Remainder 4.

$2 \times 4 = \cancel{8} = 1.$

$5 \times 5 = 25$ ie $\cancel{3 \times 7} + 4 = 4.$

$5b = 1$ what is b, b is 3 because $3 \cdot 5 = 15 = \cancel{2 \cdot 7} + 1 = 1$

__Theorem (w/out Proof)__.

For every prime # p, $F_p = \{0, 1, 2, \dots, p-1\}$ along w/ $+$ & $\times$ defined as above (ie $a, b \mapsto a+b \bmod p$) is a field.

__Theorem__ (Basic Properties of Fields) Let F be a field. and let a, b, c denote elements of F. Then:

1. __$a+b = c+b \Rightarrow a = c$__

__Proof:__ By F_4 there is some $b' \in F$ s.t. $b + b' = 0$

we have $a+b = c+b$.

$(a+b)+b' = (c+b)+b'$

$\Rightarrow a+(b+b') = c+(b+b')$ (F_2)

by the choice of b' $\{$ie $b+b'=0\}$ we have

$a+0 = c+0$

$\therefore a=c$ $[F_3]$

2. $b \neq 0$ & $a \cdot b = c \cdot b \Rightarrow a=c$

Proof: more or less same as 1

ie by F_4 $(ab)b' = (cb)b'$ wher $bb'=1$ since $b' \neq 0$..

3. If $0' \in F$ is "like 0" then it is 0. [ie $0'$ satisfies property that characterizes 0]

ie. If $0' \in F$ Satisfies $\forall a \in F$ $a+0'=a$ then $0'=0$.

(ie in a Field there is only One 0)

Proof of 3

$0'+0 = 0'$ (F_3) $= 0+0'$ (F_1) $= 0$ (by assumption on $0'$) $\square$

4. If $1'$ is "like 1" then $1'=1$, $\forall a$ $a \cdot 1 = a$.

Proof: similar to Proof of 3

5. If b & b' satisfy $a+b=0$ & $a+b'=0$ then $b=b'$.

$\Rightarrow$ in any field "$-a$" makes sense (ie unambiguos)

meaning $(-a)$: that b s.t. $a+b=0$

Proof:

$a+b = 0 = a+b'$

by F_1 $b+a = 0 = b'+a$

then by concellation law it follows $b=b'$

6. If $a \neq 0$ & $ab = 1 = ab' \Rightarrow b = b'$

Proof: similar to proof of 5. (now can use a^{-1})

7. $-(-a) = a$ & if $a \neq 0$ $(a^{-1})^{-1} = a$

Proof

(*) $a + (-a) = 0$ by defn

$(-a) + -(-a) = 0$ by defn

by (*) & F1 $(-a) + a = 0$

by the already proven "each element has unique inverse"

$-(-a)$ & a must be same.

[another way to prove this would have been to use cancellation law]