

1. If F is a field in which 0 has a multiplicative inverse, show $|F| = 1$.

Proof: Suppose $|F| > 1$, and let $x \in F$ such that $x = 0^{-1}$. Then $0x = 1 = 0$. We know that under multiplication, any element in F can be expressed as $1 \times y \forall y \in F$, and since $1 = 0$, $1 \times y = 0 \times y = 0$. Therefore the only element in F is 0, and $|F| = 1$.

2. Suppose that $n > 1$ is an integer and let \mathbb{Z}_n be equipped with addition and multiplication modulo n . Prove that \mathbb{Z}_n is a field if and only if n is prime.

In order to be a field, \mathbb{Z}_n must fulfill the following axioms:

- (A1) Addition is commutative on F .
- (A2) Addition is associative on F .
- (A3) There is a unique additive identity, called 0.
- (A4) There is an additive inverse $-a$ for all $a \in F$.
- (M1) Multiplication is commutative on F .
- (M2) Multiplication is associative on F .
- (M3) There is a unique multiplicative identity called 1.
- (M4) There is an multiplicative inverse element a^{-1} for every $a \in F$.
- (D) For all $x, y, z \in F$, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.
- (ZO) The additive and multiplicative identity are distinct.

Proof: Suppose n is prime. Then every element in \mathbb{Z}_n is a unit, so \mathbb{Z}_n is equipped with a multiplicative inverse. Since \mathbb{Z}_n has addition and multiplication, we know it is commutative and associative for both those operations. We know that \mathbb{Z}_n contains 0, so it has the additive inverse. Addition and multiplication form the distributive law, so \mathbb{Z}_n is equipped with the distributive law. Since $n > 1$, \mathbb{Z}_n $0 \neq 1$. Therefore, by definition, \mathbb{Z}_n is a field since it fulfills all the field axioms.

Suppose \mathbb{Z}_n is a field with n not prime. Since n is not prime, then we can find an element $x \in \mathbb{Z}_n$ such that $\gcd(n, x) \neq 1$. Therefore there is an element in \mathbb{Z}_n that is not a unit, so \mathbb{Z}_n is not a field, since there is an element without an inverse.

3. Suppose that F is a finite field and $x \in F \setminus \{0\}$. Prove that there exists $n \in \mathbb{N}$ such that $x^n = 1$.

Proof: Consider $x^r = x^s$ for $s \neq r \in \mathbb{N}$ where $s > r$ without loss of generality. We know that for every element in F , there is a multiplicative inverse of that element, so we define $(x^r)^{-1} = x^{-r}$. Then $x^{-r}x^r = x^{-r}x^s$ and $1 = x^{s-r}$. Since $s > r$, $s - r \in \mathbb{N}$, so we have found the n we were looking for.