Abstract Algebra

Notes - Year 1, Semester 2

Angel Cervera Roldan
21319203

Contents

Fields

A field is a set F containing at least two elements, along with two operations:

- $+ : F \times F \to F$
- $\cdot : F \times F \to F$

that satisfies the following axioms:

1. $a + b = b + a$, and $a \cdot b = b \cdot a \quad \forall a, b \in F$
2. $(a + b) + c = a + (b + c)$, and $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b \in F$
3. $\exists 0 \in F$ such that $a + 0 = a \quad \forall a \in F$
4. $\exists 1 \in F$ such that $a \cdot 1 = a \quad \forall a \in F$, where $0 \neq 1$
5. $\forall a \in F$, $\exists(-a)$ such that $a + (-a) = 0$
6. $\forall a \in F - \{0\}$, $\exists(a^{-1})$ such that $a \cdot (-a) = 1$
7. $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in F$

Theorem

$\mathbb{Z}_p$ is the set of integers mod p.
$\mathbb{Z}_p$ is a field iff p is a prime number.

From the axioms, $\forall a, b, c \in F$ the following can be proven

1. $a + b = a + c \implies b = c$
2. $a \neq 0$, $ab = ac \implies b = c$
3. $-(-a) = a$
4. $a \cdot 0 = 0$