Definition 18.1

Let R be a commutative ring. An element $a \neq 0$ of R is a *zero divisor* if there exists $b \neq 0$ such that $ab = 0$.

Definition 18.2

An *integral domain* is a commutative ring with unity which has no zero divisors.

Theorem 18.3

Let R be an integral domain and $a, b, c \in R$. If $a \neq 0$ and $ab = ac$ then $b = c$.

Definition 18.4

Let R be a commutative ring with unity. An element $a \in R$ is a *unit* if there exists $b \in R$ such that $ab = 1$. In such case, we denote $a^{-1} := b$.

Definition 18.5

A *field* is a commutative ring with unity in which every non-zero element is a unit.

Theorem 18.6

Every field is an integral domain.

Theorem 18.7

A ring $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Definition 18.8

Let F be a field with unity $1 \in F$. The *characteristic* of F is the smallest positive integer n such that

$$\underbrace{1 + 1 + \ldots + 1}_{n \text{ times}} = 0$$

denote such n by $\chi(F)$.

If such n does not exist, then $\chi(F) = 0$

Theorem 18.9

1) If F is a field then $\chi(F)$ is either 0 or a prime number.

2) If F is a finite field and $\chi(F) = p$ for some prime p, then F consists of p^n elements for some $n \geq 1$.

Note. Proof of Theorem 18.9 shows that if F is a finite field of characteristic p, and we consider F as an additive abelian group then every non-identity element of F had order p. Using Theorem 16.1 we obtain that as an abelian group F is isomorphic to $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$.

Example: Field with 9 elements.