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 $ab = 0$.

Example. In the ring $\mathbb{Z}_6$ the elements 2 and 3 are zero divisors since $2 \cdot 3 = 0$.

Definition 18.2

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

Example. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are integral domain.

Example. $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain since $(1,0) \cdot (0,1) = (0,0)$.

Theorem 18.3

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

Proof. If $ab = ac$ then $a(b - c) = 0$. Since R is an integral domain and $a \neq 0$, this means that $b - c = 0$, and so $b = c$. □

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 $a^{-1} := b$.

Example The only units in $\mathbb{Z}$ are 1 and -1.

Example Every non-zero element of $\mathbb{Q}$ is a unit.

Definition 18.5

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

Example. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

Theorem 18.6

Every field is an integral domain.

Proof. Let F be a field and $a, b \in F$ be non-zero elements. If $a \cdot b = 0$ then $b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$, which is a contradiction. □

Theorem 18.7

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

Proof. If n is not a prime number, then $n = km$ for some $1 < k, m < n$. Consider k, m as elements of $\mathbb{Z}_n$. Then $k \neq 0$, $m \neq 0$ but $k \cdot m = 0$. This shows that $\mathbb{Z}_n$ is not an integral domain and so it is not a field.

Conversely, assume that n is a prime number and that $k \in \mathbb{Z}_n$, $k \neq 0$. Then $\gcd(k, n) = 1$, so there exists $a, b \in \mathbb{Z}$ such that $ak + bn = 1$. This gives $a \cdot k = 1$ in $\mathbb{Z}_n$, so k is a unit in $\mathbb{Z}_n$ and $k^{-1} = a$. □

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 $\chi(F) = 0$

Example

- $\chi(\mathbb{Q}) = \chi(\mathbb{R}) = \chi(\mathbb{C}) = 0$

- If p is a prime number then $\chi(\mathbb{Z}_p) = p$.

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 $n \geq 1$.

Proof. **1)** Assume that $\chi(F) > 0$ and $\chi(F) = km$ for some $k, m > 1$. denote

$$\mathbf{k} = \underbrace{1 + 1 + \ldots + 1}_{k \text{ times}}$$
$$\mathbf{m} = \underbrace{1 + 1 + \ldots + 1}_{m \text{ times}}$$

Then $\mathbf{k}, \mathbf{m}$ are non-zero elements in F, since $k, m < \chi(F)$. Also:

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

since $km = \chi(F)$. This means that $\mathbf{k}$ and $\mathbf{m}$ are zero divisors, which is impossible.

2) Consider F as an abelian group with addition. For any element $a \in F$ we have

$$pa = (\underbrace{1 + 1 + \cdot + 1}_{p \text{ times}}) \cdot a = 0 \cdot a = 0$$

This means the order of a divides p, and so it is either 1 or p. By Theorem 15.6 this implies that $|F| = p^n$ 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. Here is an example of a field $\mathbb{Z}_3[i]$ of characteristic 3 with 9 elements. It is obtained by starting with the field $\mathbb{Z}_3$ and adding to it a new element i such that $i^2 = -1$. More explicitly:

$$\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$$

Addition and multiplication in $\mathbb{Z}_3[i]$ are given by

$$(a+bi)+(c+di) = (a+c)+(b+d)i$$
$$(a+bi)\cdot(c+di) = (ac-bd)+(ac+bd)i$$

We will show that all non-zero elements of $\mathbb{Z}_3[i]$ are units. Notice that the polynomial $p(x) = x^2+1$ has no roots in $\mathbb{Z}_3$. This implies that if $a, b \in \mathbb{Z}_3$ and $b \neq 0$ then $a^2+b^2 = b^2((ab^{-1})^2+1) \neq 0$. By the same argument, if $a \neq 0$ then $a^2+b^2 \neq 0$.

Take a non-zero element $a+bi \in \mathbb{Z}_3[i]$. We have

$$(a+bi)(a-bi) = a^2+b^2$$

Since, by the observation above, $a^2+b^2 \neq 0$, thus the element $(a^2+b^2)^{-1}$ exists in $\mathbb{Z}_3$ and we have

$$(a+bi)(a-bi)(a^2+b^2)^{-1} = 1$$

This shows that $(a+bi)^{-1} = (a-bi)(a^2+b^2)^{-1}$.

Example. The same procedure does not work for constructing a field with 25 elements. Take $\mathbb{Z}_5[i] = \{a+bi \mid a, b \in \mathbb{Z}_5\}$ with $i^2 = -1$. Then

$$(i-2)(i-3) = 0$$

so $\mathbb{Z}_5[i]$ is not an integral domain, and thus not a field.

The difference between $\mathbb{Z}_3[i]$ and $\mathbb{Z}_5[i]$ is that the polynomial $p(x) = x^2+1$ does not have any roots in $\mathbb{Z}_3$. By adding the element i to this field with $i^2 = -1$ we create roots of this polynomial, $x = i$ and $x = -i$.

On the other hand, in $\mathbb{Z}_5$ the polynomial $p(x) = x^2+1$ already has two roots: $x = 2$ and $x = 3$. It means that $p(x) = (x-2)(x-3)$. By adding i to $\mathbb{Z}_5$ we create an additional root $x = i$. This gives:

$$0 = p(i) = (i-2)(i-3)$$