

Exercise 13.15: Let a belong to a ring R with unity and suppose that $a^n = 0$ for some positive integer n . (Such an element is called nilpotent.) Prove that $1 - a$ has a multiplicative inverse in R . [Hint: Consider $(1 - a)(1 + a + a^2 + \cdots + a^{n-1})$.]

Note that $b = (1 + a + a^2 + \cdots + a^{n-1}) \in R$ and that $(1 - a)b = (1 + a + a^2 + \cdots + a^{n-1}) - (a + a^2 + a^3 + \cdots + a^n) = 1 - a^n = 1$ thus $b = (1 - a)^{-1}$.

Exercise 13.18: A ring element a is called an idempotent if $a^2 = a$. Prove that the only idempotents in an integral domain are 0 and 1.

Suppose R is a integral domain. Suppose that $a \notin \{0, 1\}$ and that $a^2 = a$. Note that a^{-1} exists. Note that $1 = aa^{-1} = a^2a^{-1} = aaa^{-1} = a$ a contradiction we now conclude that the only idempotents in an integral domain are 0 and 1.

Exercise 13.22: Prove that if a is a ring idempotent, then $a^n = a$ for all positive integers n .

I will proceed with proof by induction.

Note that the statement is true for $n = 1$ and true for $n = 2$.

Suppose that the statement $a^n = a$ holds for $n \geq 2$. Note that $a = a^n = aa^{n-1} = a^2a^{n-1} = a^{n+1}$. By induction we conclude that if a is a ring idempotent, then $a^n = a$ for all positive integers n .

Exercise 13.25: Find an idempotent in $Z_5[i] = \{a + bi \mid a, b \in Z_5\}$.

Note that $(3 + i)^2 = 8 + 6i = 3 + i$, thus $3 + i$ is a idempotent in $Z_5[i] = \{a + bi \mid a, b \in Z_5\}$.

Exercise 13.28: Let R be the set of all real-valued functions defined for all real numbers under function addition and multiplication.

a) Determine all zero-divisors of R .

The function f is a zero-divisors of R if there exists some $a \in \mathbb{R}$ such that $f(a) = 0$.

Suppose $f \in R - \{0\}$ and there exists $a \in \mathbb{R}$ such that $f(a) = 0$. Define

$$g(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}$$

Note that $g \neq 0$. Note that $f * g = 0$ thus f is a zero-divisors of R .

Suppose f is a never zero function. Suppose f is a zero-divisors of R . There exists $g \in R - \{0\}$ such that $f * g = 0$. There exists $a \in \mathbb{R}$ such that $g(a) \neq 0$. Note that $f * g(a) = f(a) * g(a) \neq 0$ thus we have a contradiction and we conclude that no never zero functions are zero-divisors of R .

b) Determine all nilpotent elements of R .

Suppose $f \in R - \{0\}$ and f is a nilpotent element of R . There exists some n such that $f^n = 0$. Note that there exists $a \in \mathbb{R}$ such that $f(a) \neq 0$. Note that $f^n(a) = (f(a))^n \neq 0$ a contradiction conclude that only 0 is a nilpotent element of R .

c) Show that every nonzero element is a zero-divisor or a unit.

Suppose f is a nonzero element. Suppose f is not a zero-divisor. Note that f is a never

zero function. Define a function $g(x) = 1/f(x)$. Note that $f * g = 1$. Conclude f is a unit. Conclude that every nonzero element is a zero-divisor or a unit.

Exercise 13.31: Let R be a ring with unity 1. If the product of any pair of nonzero elements of R is nonzero, prove that $ab = 1$ implies $ba = 1$.

Suppose $ab = 1$. Note that $(ba)b = b(ab) = b$ and thus $ba = 1$.

Exercise 13.35: Let F be a field of order 2^n . Prove that $\text{char } F = 2$.

Suppose that $(\nexists a \neq 0)a = -a$. In this case we can pair off non-zero elements each with their additive inverse. This means that there are an even number of non-zero elements, or that the total number of elements is odd, a contradiction with the total number of elements being 2^n .

We know there must exist some $a \in F - \{0\}$ such that $a = -a$. Note that $a(1 + 1) = a + a = a + (-a) = 0$ implies that $1 + 1 = 0$ and thus $\text{char } F = 2$.

Exercise 13.51: Show that any finite field has order p^n , where p is a prime. Hint: Use facts about finite Abelian groups. (This exercise is referred to in Chapter 22.)

Suppose F is a finite field. Suppose $|F|$ is not a prime to a power. Note that $6 \leq |F| = abc$ where a, b are distinct primes. There must exist an element in the finite abelian group F under $+$ such that $|A|_+ = a$, and another element such that $|B|_+ = b$. Note that $aA = A + A + \cdots + A = 0$ implies $A(1 + 1 + \cdots + 1) = 0$ and thus since A is clearly non zero $a1 = 0$ or in other words $|1|_+ \mid a$ and likewise $|1|_+ \mid b$. Note that $|1|_+ \mid \gcd(a, b) = 1$ thus $|1|_+ = 1$ thus $1 = 0$ a contradiction, conclude that $|F| = p^n$ for some prime p and some natural n .