Adam Jump
Rings and Fields
Chapter 13

3. Show that a commutative ring with the cancellation property (under multiplication) has no zero-divisors.

Let R be a commutative ring with the cancellation property and arbitrary elements a, b, c.
For the sake of demonstration, let $a \neq 0$, $ab = 0$, and $ac = 0$. So $ab = ac$ implies $b = c$ which is not true if the ring has at least two zero divisors.

5. Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.

Let $a, b \in \mathbb{Z}_n$ where $a, b \neq 0$. We can see that $ab \mod n$ reduces to $kn - kr \mod n$ for some $k \in \mathbb{N}$ and $r \in \mathbb{Z}_n$. Now we must show that $kn - kr \mod n$ is either 0 or 1. First of all, we can see that $kn \mod n = 0$, which means that $-kr \mod n$ is the only expression left to deal with. If n is prime, then $-kr \neq n$, and so $-kr \mod n \neq 0$; this means that $-kr$ is an element of a field, $\mathbb{Z}_p$ and must be a unit. Otherwise, if n is not prime, then $-kr$ must have a complementary multiple, q, such that $-krq = n$, or $-krq \mod n = n \mod n = 0$.

6. Find a nonzero element in a ring that is neither a zero-divisor nor a unit.

In the ring of integers $\mathbb{Z}$, we can see that 2 is not a zero-divisor, nor a(n) unit.

11. Let d be an integer. Prove that $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ is an integral domain. (This exercise is referred to in Chapter 18.)

By definition of integral domain, $\mathbb{Z}[\sqrt{d}]$ must have no zero divisors. Let $a + b\sqrt{d}, c + e\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. If , $\mathbb{Z}[\sqrt{d}]$ is an integral domain, then $(a + b\sqrt{d})(c + e\sqrt{d}) = ac + (ae + bc)\sqrt{d} + bed \neq 0$. If $\sqrt{d}$ is equal to 0, then a and c must be nonzero, which means ac is nonzero; otherwise $\mathbb{Z}$ would have zero divisors. If $\sqrt{d}$ is not equal to 0, then we must show that ae is not the additive inverse of bc, and concurrently that ac is not the additive inverse of bed.

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. [Hints Consider $(1 - a)(1 + a + a^2 + \cdots + a^{n-1})$.]

Using the provided hint, we see that $(1-a)(1+a+a^2+\cdots+a^{n-1}) = 1+a+a^2+\cdots+a^{n-1}-a-a^2-\cdots-a^n$. Which reduces to $1 - a^n$, where $a^n = 0$ which means that $(1 - a)(1 + a + a^2 + \cdots + a^{n-1}) = 1$, and that $1 - a$ is a unit of R.
16. Show that the nilpotent elements of a commutative ring form a subring.

Let R be a commutative ring with arbitrary nilpotent elements a, b; let S be a subset of R containing only nilpotent elements. Show $a - b, ab \in S$.
We know that $a^n - b^n \in S$ which implies that $(a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}) \in S$. This shows that $(a - b) \in S$.
Now, $a^n b^n \in S$, which means that $ab(a^{n-1}b^{n-1})$ (as R is commutative) is an element of S as well.

21. Let R be the ring of real-valued continuous functions on $[-1, 1]$. Show that R has zero-divisors.

Let $f(x) = \begin{cases} \sin(x) & -1 \leq x < 0 \\ 0 & x \geq 0 \end{cases}$ and $g(x) = \begin{cases} 0 & -1 \leq x < 0 \\ \sin(x) & x \geq 0 \end{cases}$, we can see that $f(x)g(x) = 0$ for all x in $[-1, 1]$.

29. (Subfield Test) Let F be a field and let K be a subset of F with at least two elements. Prove that K is a subfield of F if, for any $a, b([b \neq 0)$ in K, $a - b$ and ab^{-1} belong to K.

By the one step subgroup test, we can see that $a - b$ is true. Because ab^{-1} is an element of F, ab^{-1} must be an element of K as well.

34. Prove that there is no integral domain with exactly six elements. Can your argument be adapted to show that there is no integral domain with exactly four elements? What about 15 elements? Use these observations to guess a general result about the number of elements in a finite integral domain.

Every finite integral domain is a field. The group of this ring is isomorphic to $\mathbb{Z}_6$, as it must be a finite abelian group. Under multiplication, $\mathbb{Z}_6$ has zero divisors (e.g. $2 \cdot 3 \mod 6 = 0$). This extends to integral domains with 4 and 15 elements, which implies that every finite integral domain must have a prime number of elements.

56. Find all solutions of $x^2 - x + 2 = 0$ over $\mathbb{Z}_3[i]$. (See Example 9.)

We can see that $2 + i$, $2 + 2i$ are the only solutions to the equation $x^2 - x + 2 = 0$ over $\mathbb{Z}_3[i]$.

61. Describe the smallest subfield of the field of real numbers that contains $\sqrt{2}$. (That is, describe the subfield K with the property that K contains $\sqrt{2}$ and if F is any subfield containing $\sqrt{2}$, then F contains K.)

As a result of having multiplicative inverses, we have $1/\sqrt{2}$ which means we have 1, which generates $\mathbb{N}$. Likewise, we have $1/\sqrt{2} \cdot 1/\sqrt{2}$, or $1/2$, and so we have $\mathbb{Q}$. Now, the only irrational number we have is $\sqrt{2}$, which means that the smallest subfield of the reals containing $\sqrt{2}$ is $\mathbb{Q}[\sqrt{2}] = \left\{ \frac{a}{b} \cdot \sqrt{2} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$

67. Suppose that D is an integral domain and that ϕ is a nonconstant function from D to the nonnegative integers such that $\phi(xy) = \phi(x)\phi(y)$. If x is a unit in D, show that $\phi(x) = 1$.

We know that x is a unit of D, and that there exists some $b \in D$ such that $xb = 1_D$. Now, by evaluating $\phi(xb) = \phi(1_D) = 1$, we can say that $\phi(xb) = \phi(x)\phi(b) = 1$, which really means that both x and b are mapped to 1 under ϕ.