Solution Outlines for Chapter 13

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

Consider the polynomial ring $\mathbb{Z}[x]$. Then $x \in \mathbb{Z}[x]$ but it is not a zero divisor and it is not a unit.

10: Describe all zero-divisors and units of $\mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}$.

The zero divisors are elements with one or two entries that are zero. Formally, $\{(a, b, c) | \text{exactly 1 or 2 of }$

The units are elements composes of units so they have ± 1 in the first and last coordinate, and the middle coordinate is not 0. So $\{(\pm 1, b, \pm 1) | b \neq 0\}$.

12: In \mathbb{Z}_7 give a reasonable interpretation for the expressions $\frac{1}{2}$, $-\frac{2}{3}$, $\sqrt{-3}$, and $-\frac{1}{6}$.

Since 2 * 4 = 8 = 1, $4 = \frac{1}{2}$. Since 3 * 5 = 15 = 1, 5 acts like $\frac{1}{3}$. So $-\frac{2}{3} = -1 + \frac{1}{3} = 6 + 5 = 11 = 4$. [Alternately, $\frac{2}{3} = 2 * 5 = 3$, so $-\frac{2}{3} = -3 = 4$.] Now, -3 = 4 so $\sqrt{-3} = \sqrt{4} = 2$. Finally, 6 * 6 = 36 = 1 so $\frac{1}{6} = 6$ and $-\frac{1}{6} = -6 = 1$.

13: Give an example of a commutative ring without zero-divisors that is not an integral domain.

 $2\mathbb{Z}$ (Note: this is a commutative ring without zero-divisors and without unity)

16: Show that the nilpotent elements of a commutative ring form a subring.

Let N be the set of nilpotent elements of a commutative ring. This is non-empty since $0^1 = 0$. Now, let $a, b \in N$. Then there exists an $n, m \in \mathbb{Z}_{>0}$ such that $a^n = 0 = b^m$. So $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = (0)(0) = 0$ so $ab \in N$ (Note: we could actually use lcm(n,m) instead of nm). Now $(a-b)^{n+m} = \sum_{k=0}^{n+m} {n+m \choose k} (-1)^k a^k b^{n+m-k}$. We notice that for $n \leq k \leq n+m, a^k = a^n a^{k-n} = 0$. For $0 \leq a < n, b^{n+m-k} = b^m b^{n-k} = 0$. Thus the sum is 0 and $a-b \in N$.

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

Let a be an idempotent in an integral domain. Then $a^2 = a$ so $a^2 - a = a(a - 1) = 0$. Since there are no zero divisors in an integral domain, a = 0 or a - 1 = 0. Thus a = 0 or a = 1.

26: Find all units, zero-divisors, idempotents, and nilpotent elements in $\mathbb{Z}_3 \oplus \mathbb{Z}_6$.

Units: (1, 1), (2, 1), (1, 5), (2, 5)Zero-divisors: (0, 2), (0, 3), (0, 4), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)Idempotents: (0, 0), (0, 1), (0, 3), (0, 4), (1, 0), (1, 1), (1, 3), (1, 4) Nilpotent elements: (0,0)

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.

Notice that this is the subgroup test under addition and the subgroup test under multiplication (excluding 0). Thus it is closed under addition, multiplication, additive inverses, and multiplicative inverses. Hence it is a subring where every non-zero element has a multiplicative inverse, or a field. Note, the commutative part of field is inherited.

35: Let F be a field of order 2^n . Prove that char F = 2.

Let F be a field of order 2^n . We know that the *char* F = |1|. Since the order of the field is 2^n , the order of 1 divides 2^n . But F is a field and all fields are integral domains. By Theorem 13.3, we know that the characteristic of an integral domain is either 0 or prime. Hence, the characteristic of F is a prime that divides 2^n . Thus *char* F = 2.

41: If a is an idempotent in a commutative ring, show that 1 - a is also an idempotent.

Let a be an idempotent in a commutative ring. Then $a^2 = a$. Hence, $(1 - a)^2 = 1 - 2a + a^2 = 1 - 2a + a = 1 - a$. So 1 - a is also an idempotent.

46: Suppose that a and b belong to a commutative ring and ab is a zero-divisor. Show that either a or b is a zero-divisor.

Let a and b belong to a commutative ring and ab be a zero-divisor. Then there is a $c \neq 0$ such that (ab)c = 0. Observe that $ab \neq 0$ implies that $a \neq 0$ and $b \neq 0$. Suppose that a is not a zero divisor. Then a(bc) = 0 implies that bc = 0 but this means that b is a zero-divisor. Hence, either a or b is a zero-divisor.

#47: Suppose that R is a commutative ring without zero-divisors. Show that all the nonzero elements of R have the same additive order.

Let R be a commutative ring without zero-divisors (note: this may not be an integral domain because it may not have unity). Let the additive order of a nonzero element x be n and the additive order of another nonzero element y be m where $n \neq m$. Without loss of generality, assume n < m. Then 0 = (nx)y = x(ny). Since there are no zero divisors, and $x \neq 0, ny = 0$. But this is a contradiction.

57: Consider the equation $x^2 - 5x + 6 = 0$.

First notice: $x^2 - 5x + 6 = (x - 2)(x - 3)$.

- a. How many solutions does this equation have in \mathbb{Z}_7 ? 2 (specifically, 2 and 3)
- b. Find all solutions of this equation in \mathbb{Z}_8 . 2, 3

- c. Find all solutions of this equation in \mathbb{Z}_{12} . 2, 3, 6, 11
- d. Find all solutions of this equation in \mathbb{Z}_{14} . 2, 3, 9, 10

68: Let F be a field of order 32. Show that the only subfields of F are F itself and $\{0, 1\}$.

Let F be a field of order 32. Then there are 31 non-zero elements in F. Recall the non-zero elements must be a subgroup under multiplication in order to have a subfield. Hence, we can apply Lagrange's theorem. So the number of non-zero elements in the subfield must be 1 or 31. These would be the subgroups $\{1\}$ and F^* respectively. Hence, the only subfields are $\{1, 0\}$ and $F^* \cup \{0\} = F$.