Solution Outlines for Chapter 12

 # 3: Give an example of a subset of a ring that is a subgroup under addition but not a subring.

In $\mathbb{C}$, $\{bi|b \in \mathbb{Z}\}$ is a subgroup but not a subring since $i^2 = -1 \notin \{bi\}$. Similarly, in $\mathbb{R}$, $\{n\sqrt{2}|n \in \mathbb{Z}\}$ is a subgroup but not a subring.

 # 4: Show, by example, that for any fixed nonzero elements a and b in a ring, the equation $ax = b$ can have more than one solution. How does this compare with groups?

Consider the ring $\mathbb{Z}_4$, let $a = b = 2$. Then $2(1) = 2$ and $2(3) = 2$ so $2x = 2$ has two solutions. This is in contrast to groups where there is only one solution, $x = a^{-1}b$.

 # 6: Find an integer n that shows that the rings $\mathbb{Z}_n$ need not have the following properties that the ring of integers has. Then answer: Is the n you found prime?

1. $a^2 = a$ **implies** $a = 0$ **or** $a = 1$**.** Let $n = 6$. Then $3^2 = 3$ but 3 is neither 0 nor 1.
2. $ab = 0$ **implies** $a = 0$ **or** $b = 0$**.** Let $n = 6$. Then $2 \cdot 3 = 0$ but $2 \neq 0$ and $3 \neq 0$.
3. $ab = ac$ **and** $a \neq 0$ **implies** $b = c$**.** Let $n = 6$. $3 \cdot 2 = 0 = 3 \cdot 4$ but $3 \neq 0$ and $2 \neq 4$.

 # 9: Prove that the intersection of any collection of subrings of a ring R is a subring of R.

Let G be the intersection of any collection of subrings. Notice that the intersection must include 0 so it is a non-empty set. Let a and b be elements of G. Then a and b are in each ring. Thus $a - b$ and ab are in each ring. But since these are in every ring, $a - b$ and ab are also in the intersection. Hence it is a subring.

 # 12: Let a, b, and c be elements of a commutative ring, and suppose that a is a unit. Prove that b divides c if and only if ab divides c.

Let a, b, and c be elements of a commutative ring where a is a unit. Suppose that b divides c. Then $c = bd$ for some d in the ring. Then $c = ab(a^{-1}d)$ where $a^{-1}d$ is in the ring. Hence ab divides c. Suppose instead that ab divides c. Then $abd = c$ for some d in the ring. So $b(ad) = c$ so b divides c.

 # 17: Show that a ring that is cyclic under addition is commutative.

Suppose that R is a ring that is cyclic under addition. Call its additive generator a. Then any element in R is of the form na for some $n \in \mathbb{Z}$. Farther, $(na)(ma) = (nm)a^2 = (ma)(na)$ by exercise 15. Hence R is commutative.

 # 19: Let R be a ring. The *center of* R is the set $\{x \in R \big| ax = xa$ for all a in $R\}$. Prove that the center of a ring is a subring.

Clearly 0 is in the center since $0x = 0 = x0$ for all $x \in R$. Hence the center is non-empty. Now, let a and b be elements of the center of R. Then $(a-b)x = ax - bx = xa - xb = x(a-b)$ so $a - b$ is in the center. Similarly, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ so ab is in the center. Hence, the center of a ring is a subring.

 # 20: Describe the elements of $M_2(\mathbb{Z})$ that have multiplicative inverses.

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $M_2(\mathbb{Z})$. Then A has a multiplicative inverse iff it has non-zero determinant so $ad - bc \neq 0$. Moreover, the inverse is only in $M_2(\mathbb{Z})$ if the $\frac{1}{det(A)}$ is in $\mathbb{Z}$ (in order to ensure that the matrix entries are all integers). Thus the determinant of A must be ± 1. Thus the elements with multiplicative inverse are $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| ad - bc = \pm 1 \right\}$.

 # 27: Show that a unit of a ring divides every element of the ring.

Let a be a unit in a ring R. Let x be any element in R. Then $x = aa^{-1}x = a(a^{-1}x)$, and $a^{-1}x$ is also in R. Hence a divides x.

 # 31: Give an example of ring elements a and b with the properties that $ab = 0$ but $ba \neq 0$.

Let $R = M_2(\mathbb{Z})$. Then $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0$ but $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

 # 33: Suppose that R is a ring such that $x^3 = x$ for all x in R. Prove that $6x = 0$ for all x in R.

Let R be a ring such that $x^3 = x$ for all $x \in \mathbb{R}$. Then, for any x, $(2x)^3 = 2x$ and $8x^3 = 8x$ Hence, $2x = 8x$ so $6x = 0$.

 # 38: Is $\mathbb{Z}_6$ a subring of $\mathbb{Z}_{12}$?

No: The operations in $\mathbb{Z}_6$ are different than the ones in $\mathbb{Z}_{12}$.

 # 42: Let $R = \{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} | a, b \in \mathbb{Z}\}$. Prove or disprove that R is a subring of $M_2(\mathbb{Z})$.

Note it is clear that $R \subseteq M_2(\mathbb{Z})$ and since R contains the zero matrix (among many others), R is non-empty. Let $A = \begin{bmatrix} a & a \\ b & b \end{bmatrix}$ and $C = \begin{bmatrix} c & c \\ d & d \end{bmatrix}$ be matrices in R. Then $A - B = \begin{bmatrix} a-c & a-c \\ b-d & b-d \end{bmatrix}$, which is in R since the integers are closed under subtraction. Additionally, $AC = \begin{bmatrix} ac+ad & ac+ad \\ bc+bd & bc+bd \end{bmatrix}$. Since $ac+ad$ and $bc+bd$ are in $\mathbb{Z}$, $AC \in R$. Since R is closed under subtraction and multiplication, R is a subring.

 # 43: Let $R = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ and $S = \{(a, b, c) \in \mathbb{R} | a + b = c\}$. Prove or disprove that S is a subring of R.

First, it is clear that S is contained in R and that S is not empty (S contains $(0,0,0)$). Let $x = (a,b,c)$ and $y = (d,f,g)$ be elements of S. Then $x - y = (a,b,c) - (d,f,g) = (a-d, b-f, c-g)$. Since $x, y \in S$, $a + b = c$ and $d + f = g$. Now, $(a-d) + (b-f) = (a+b) - (d+f) = c - g$ so $x - y \in S$. Now, consider the condition for $xy = (ad, bf, cg)$. We have that $cg = (a+b)(d+f) = ad + bf + af + bd$ so xy is in S only if $af + bd = 0$. But this equality is not always true. For example, let $x = (1,2,3)$ and $y = (4,5,9)$. Then $xy = (4,10,27)$ but $4+10 \neq 27$. Hence we can not say that $xy \in S$. Thus, S is not a subring of R.

 # 45: Let R be a ring with unity 1. Show that $S = \{n \cdot 1 \big| n \in \mathbb{Z}\}$ is a subring of R.

We know that S is non-empty since $1 \cdot 1 = 1$ is in S. Now, let $a, b \in \S$. Then $a = x \cdot 1$ and $b = y \cdot 1$ for some $x, y \in \mathbb{Z}$. So $a - b = x \cdot 1 - y \cdot 1 = (x-y) \cdot 1$ so $x - y \in S$. Additionally, $ab = (x \cdot 1)(y \cdot 1) = (xy) \cdot 1$ so $ab \in S$.

 # 46: Show that $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.

Notice that 2 and 3 are both in $2\mathbb{Z} \cup 3\mathbb{Z}$ but $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

 # 50: Suppose that R is a ring and that $a^2 = a$ for all a in R. Show that R is commutative. (Note: Such a ring is called a Boolean ring.)

Let R be a ring such that $a^2 = a$ for all $a \in R$. We notice that $a+b = (a+b)^2 = a^2+b^2+ab+ba = a+b+ab+ba$. Thus $ab+ba = 0$, or $ab = -ba$. Now $-ba = (-ba)^2 = (ba)^2 = ba$ so $ab = ba$, and R is commutative.