# Homework #2 Solutions

pp 254-257: 18, 34, 36, 50, 54

**p 241, #18** We apply the subring test. First of all, $S \neq \emptyset$ since $a \cdot 0 = 0$ implies $0 \in S$. Now let $x, y \in S$. Then $a(x - y) = ax - ay = 0 - 0 = 0$ and $a(xy) = (ax)y = 0 \cdot y = 0$ so that $x - y, xy \in S$. Therefore $S$ is a subring of $R$.

**p 242, #38** $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ is *not* a subring of $\mathbb{Z}_{12}$ since it is not closed under addition mod 12: $5 + 5 = 10$ in $\mathbb{Z}_{12}$ and $10 \notin \mathbb{Z}_6$.

**p 243, #42** Let $X = \begin{pmatrix} a & a \\ b & b \end{pmatrix}, Y = \begin{pmatrix} c & c \\ d & d \end{pmatrix} \in R$. Then

$$X - Y = \begin{pmatrix} a-c & a-c \\ b-d & b-d \end{pmatrix} \in R$$

since $a - c, b - d \in \mathbb{Z}$. Also

$$XY = \begin{pmatrix} ac+ad & ac+ad \\ bc+bd & bc+bd \end{pmatrix} \in R$$

since $ac + ad, bc + bd \in \mathbb{Z}$. Since $R$ is clearly nonempty, the subring test implies that $R$ is indeed a subring of $M_2(\mathbb{Z})$.

**p 254, #4** The zero divisors in $\mathbb{Z}_{20}$ are $2, 4, 5, 6, 8, 10, 12, 14, 15, 16$ and $18$, since

$$\begin{aligned}
2 \cdot 10 &= 0 \bmod 20 \\
4 \cdot 15 &= 0 \bmod 20 \\
6 \cdot 10 &= 0 \bmod 20 \\
8 \cdot 5 &= 0 \bmod 20 \\
12 \cdot 5 &= 0 \bmod 20 \\
14 \cdot 10 &= 0 \bmod 20 \\
16 \cdot 5 &= 0 \bmod 20 \\
18 \cdot 10 &= 0 \bmod 20
\end{aligned}$$

and every nonzero element not in this list is a unit. In particular this shows that the zero divisors in $\mathbb{Z}_{20}$ are precisely the nonzero nonunits. This statement generalizes to every $\mathbb{Z}_n$ (Why?).

**p 254, #6** According to the final statement of the preceding problem, we'll need to look outside of $Z_n$. An easy place to look is $\mathbb{Z}$. Indeed, any element other than $0, \pm 1$ is nonzero, not a unit, and not a zero-divisor.

**p 255, #18** The element $3+i$ is a zero divisor in $\mathbb{Z}_5[i]$ since

$$(3+i)(2+i) = 5+5i = 0+0i$$

after reducing the coefficients mod 5.

**p 255, #20** By a previous homework exercise

$$U(\mathbb{Z}_3 \oplus \mathbb{Z}_6) = U(\mathbb{Z}_3) \oplus U(\mathbb{Z}_6) = \{1,2\} \oplus \{1,5\} = \{(1,1),(1,5),(2,1),(2,5)\}.$$

The zero divisors in $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ come in two flavors: $(0,a)$ for $a = 1,2,3,4,5$ and $(b,c)$ where $b = 1,2$ and $c = 0,2,3,4$, for a total of 13 elements. The idempotents satisfy $(a,b)^2 = (a^2,b^2) = (a,b)$. Therefore, $a^2 = a$ in $\mathbb{Z}_3$ and $b^2 = b$ in $\mathbb{Z}_6$. It is easy to see that this means $a = 0,1$ and $b = 0,1,3,4$, which gives 8 idempotents. Finally, the nilpotent elements satisfy $(a,b)^n = (a^n,b^n) = (0,0)$ for some $n \in \mathbb{Z}^+$. But $a^n = 0$ has no solutions in $\mathbb{Z}_3$ other than $a = 0$ and $b^n = 0$ has has no solution in $\mathbb{Z}_6$ other than $b = 0$. Hence $(0,0)$ is the only idempotent.

**p 256, #30** Let $D$ be an integral domain and let $x \in D$ so that $x$ is its own inverse. Then $x^2 = 1$, which is the same as $x^2 - 1 = 0$. Factoring yields $(x-1)(x+1) = 0$ and since $D$ is a domain this means $x - 1 = 0$ or $x + 1 = 0$, i.e. $x = \pm 1$.

**p 256, #34** Direct computation yields

| | $0+0i$ | $1+0i$ | $0+1i$ | $1+1i$ |
|---|---|---|---|---|
| $0+0i$ | $0+0i$ | $0+0i$ | $0+0i$ | $0+0i$ |
| $1+0i$ | $0+0i$ | $1+0i$ | $0+1i$ | $1+1i$ |
| $0+1i$ | $0+0i$ | $0+1i$ | $1+0i$ | $1+1i$ |
| $1+1i$ | $0+0i$ | $1+1i$ | $1+1i$ | $0+0i$ |

proving that $\mathbb{Z}_2[i]$ is neither an integral domain nor a field, since $1+1i$ is a zero divisor.

**p 256, #36** We prove only the general statement: $\mathbb{Z}_p[\sqrt{k}]$ is a field if and only if the equation $x^2 = k$ has no solution in $\mathbb{Z}_p$. For one direction, suppose that $x^2 = k$ has no solution in $\mathbb{Z}_p$. We will show that every nonzero element in $\mathbb{Z}_p[\sqrt{k}]$ has an inverse. Let $a + b\sqrt{k} \in \mathbb{Z}_p[\sqrt{k}]$ be nonzero. If $b = 0$ then $a \neq 0$ and $a + b\sqrt{k} = a$, which has an inverse in $\mathbb{Z}_7$, hence in $\mathbb{Z}_7[\sqrt{k}]$. If $b \neq 0$ then $a^2 - b^2k \neq 0$ in $\mathbb{Z}_p$, for otherwise we would have $k = (ab^{-1})^2$, with $ab^{-1} \in \mathbb{Z}_p$. So $c = (a^2 - b^2k)^{-1}$ exists in $\mathbb{Z}_p$ and $ac - bc\sqrt{k}$ is an element of $\mathbb{Z}_p[\sqrt{k}]$ which satisfies

$$(a + b\sqrt{k})(ac - bc\sqrt{k}) = (a^2c - b^2ck) + 0\sqrt{k} = c(a^2 - b^2k) = 1$$

by the definition of $c$. Therefore, $a + b\sqrt{k}$ has an inverse. Having shown that the arbitrary nonzero element has an inverse, we conclude that $\mathbb{Z}_p[\sqrt{k}]$ is a field when $x^2 = k$ has no solution in $\mathbb{Z}_p$.

For the converse, we prove that if $x^2 = k$ has a solution in $\mathbb{Z}_p$ then $\mathbb{Z}_p[\sqrt{k}]$ is not an integral domain and therefore is not a field. Let $a \in Z_p$ satisfy $a^2 = k \bmod p$. Let $x = a + (p-1)\sqrt{k}$ and $y = a + \sqrt{k}$. Then neither $x$ nor $y$ is zero in $\mathbb{Z}_p[\sqrt{k}]$ yet

$$xy = (a^2 + k(p-1)) + (a(p-1) + a)\sqrt{k} = (a^2 - k) + (a - a)\sqrt{k} = 0 + 0\sqrt{k}$$

where we have reduced the coefficients mod $p$ at each step. Thus, $\mathbb{Z}_p[\sqrt{k}]$ possesses zero divisors and is not a field.

**p 257, #50** The characteristic is 0 since for any $n \in \mathbb{Z}^+$ we have $n \cdot (0, 4) = (0, 4n)$ and $4n$ will never be zero in $\mathbb{Z}$.

**p 257, #54** First of all, we know from previous work that $U(F)$ is a multiplicative group. But, since $F$ is a field, $U(F) = F \setminus \{0\}$. Therefore, since $F$ has $n$ elements, $F \setminus \{0\} = U(F)$ is a finite group with $n - 1$ elements. Since the order of an element in a finite group divides the order of the group itself, we see that for any nonzero $x \in F$ we have $x^{n-1} = 1$. Note that if we multiply both sides of this equation by $x$ we get $x^n = x$, which is an equation satisfied by *every* element of $F$.