Solution Outlines for Chapter 15

 # 11: Prove that the intersection of any collection of subfields of a field F is a subfield of F.

We know that every field contains 1 and 0, so the intersection of subfields is non-empty. Since a, b are in the intersection means that a, b is in each subfield, ab and $a - b$ are in each subfield. Hence the intersection is an additive subgroup and is closed under multiplication. The only other thing to check that is not inherited is that every element in the intersection has a multiplicative inverse in the intersection but this is clear because the inverse must be in each subfield.

 # 12: Let $\mathbb{Z}_3[i] = \{a + bi | a, b \in \mathbb{Z}_3\}$. Show that the field $\mathbb{Z}_3[i]$ is ring-isomorphic to the field $\mathbb{Z}_3[x]/ < x^2 + 1 >$.

Define $\phi(a + bi) = a + bi + < x^2 + 1 >$. Then $\phi((a + bi) + (c + di)) = \phi((a + c) + (b + d)i) = (a+c)+(b+d)i+ < x^2+1 >= (a+bi)+(c+di)+ < x^2+1 >= (a+bi+ < x^2+1 >)+(c+di)+ < x^2 + 1 >= \phi(a + bi) + \phi(c + di)$. Farther, $\phi((a + bi)(c + di)) = \phi((ac - bd) + (ad + bc)i) = (ac - bd) + (ad + bc)i+ < x^2 + 1 >= (a + bi)(c + di)+ < x^2 + 1 >= ((a + bi)+ < x^2 + 1 >)((c + di)+ < x^2 + 1 >)$. Hence, ϕ is a ring homomorphism.

 # 15: Consider the mapping from $M_2(\mathbb{Z})$ into $\mathbb{Z}$ given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto a$. Prove or disprove that this is a ring homomorphism.

The map is not a ring homomorphism. While addition is preserved, multiplication is not. To see this observe: $\phi(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} f & g \\ h & i \end{bmatrix}) = \phi(\begin{bmatrix} af + bh & * \\ * & * \end{bmatrix}) = af + bh \neq af = \phi(\begin{bmatrix} a & b \\ c & d \end{bmatrix})\phi(\begin{bmatrix} f & g \\ h & i \end{bmatrix})$.

 # 16: Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} | a, b, c \in \mathbb{Z} \right\}$. Prove or disprove that the mapping $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mapsto a$ is a ring homomorphism.

This map is a ring homomorphism. Addition is preserved because $\phi(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} d & f \\ 0 & g \end{bmatrix}) = \phi(\begin{bmatrix} a + d & b + f \\ 0 & c + g \end{bmatrix}) = a + d = \phi(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}) + \phi(\begin{bmatrix} d & f \\ 0 & g \end{bmatrix})$. Farther, the multiplication is preserved since $\phi(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} f & g \\ 0 & i \end{bmatrix}) = \phi(\begin{bmatrix} af & * \\ * & * \end{bmatrix}) = af = \phi(\begin{bmatrix} a & b \\ c & d \end{bmatrix})\phi(\begin{bmatrix} f & g \\ h & i \end{bmatrix})$.

 # 17: Is the mapping from $\mathbb{Z}_5$ to $\mathbb{Z}_{30}$ given by $x \mapsto 6x$ a ring homomorphism? Note that the image of the unity is the unity of the image but not the unity of $\mathbb{Z}_{30}$.

The mapping is a ring homomorphism. Addition is straightforward to show since $\phi(x+y) = 6(x+y) = 6x + 6y = \phi(x) + \phi(y)$. For multiplication, $\phi(xy) = 6xy$ and $\phi(x)\phi(y) = 6x6y = 36xy = 6xy$. Thus multiplication is preserved.

20: Recall that a ring element a is called an idempotent if $a^2 = a$. Prove that a ring homomorphism carries an idempotent to an idempotent.

Let a be an idempotent of a ring R. Then $\phi(a) = \phi(a^2) = (\phi(a))^2$. Hence, $\phi(a)$ is an idempotent.

21: Determine all ring homomorphisms from $\mathbb{Z}_6$ to $\mathbb{Z}_6$. Determine all ring homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{30}$.

Part 1: We know that a ring homomorphism must be a group homomorphism as well. Hence we know that the image of 1 has order 1, 2, 3 or 6. For the image to have order 1, $1 \mapsto 0$ and this map clearly preserves multiplication. For the order to be 2, $1 \mapsto 3$. Now $\phi(xy) = 3xy$ and $\phi(x)\phi(y) = 9xy = 3xy$ so this is indeed a ring homomorphism as well. In the order three case, 1 maps to either 2 or 4. We observe that in the first instance $\phi(xy) = 2xy \neq 4xy = \phi(x)\phi(y)$ so this is not a homomorphism. However, in the second instance $\phi(xy) = 4xy$ and $\phi(x)\phi(y) = 16xy = 4xy$ so it is a ring homomorphism. Finally, for the image to have order 5, the element 1 maps to either 1 or 5. If it maps to 1, then this is the identity map and is clearly a ring homomorphism. However, if it maps to 5, $\phi(xy) = 5xy$ but $\phi(x)\phi(y) = 25xy = xy$ so it is not a ring homomorphism. Hence the ring homomorphisms are those determined by $1 \mapsto 0$, $1 \mapsto 3$, $1 \mapsto 4$ and $1 \mapsto 1$.

Part 2: We can use a similar logic for this part. Doing this shows that the homomorphisms are those defined by 1 maps to 0, 6, 15 or 21.

30: Prove that the sum of the squares of three consecutive integers can not be a square.

Let n be an integer. Then the sum of the squares of three consecutive integers can be represented as $n^2 + (n+1)^2 + (n+2)^2$. Now consider this expression modulus 3. Then it is $n^2 + n^2 + 2n + 1 + n^2 + 4n + 4 = 3n^2 + 6n + 5 = 2$. For this expression to be a square then there must exist an element, x, in $\mathbb{Z}_3$ such that $x^2 = 2$. But $0^2 = 0$, $1^2 = 1$ and $2^2 = 1$ so there is no such solution.

37: Show that no integer of the form $111, 111, 111, \ldots, 111$ is prime.

Consider ϕ_3 as defined in class. Then $\phi_3(111, 111, 111, \ldots, 111) = \phi_3(1 \cdot 10^k + 1 \cdot 10^{k-1} +$

$\ldots + 1 \cdot 10 + 1) = \sum_{i=0}^{k} \phi_3(1)\phi_3(10)^i = \sum_{i=0}^{k} 1 \cdots 1 = 1 + 1 + 1 \cdots + 1$ but the 1's come in threes so this expression is 0 in $\mathbb{Z}_3$. Hence 3 divides the integer so it can not be prime.

 # 39: Suppose n is a positive integer written in the form $n = a_k 3^k + a_{k-1} 3^{k-1} + \cdots + a_1 3 + a_0$, where each of the a_i's is 0, 1, or 2. Show that n is even if and only if $a_k + a_{k-1} + \cdots + a_1 + a_0$ is even.

Consider ϕ_2 as defined in class. Then $\phi_2(n) = \phi_2(a_k 3^k + a_{k-1} 3^{k-1} + \cdots + a_1 3 + a_0) = \sum_{i=1}^{k} \phi_2(a_i)\phi_2(3)^i = \sum_{i=1}^{k} \phi_2(a_i) \cdot 1 = \phi_2(a_0 + a_1 + a_2 + \ldots + a_k)$. Hence, n is even iff the sum of its coefficients is even.

 # 45: Is there a ring homomorphism from the reals to some ring whose kernel is the integers?

No. The kernel of a ring homomorphism is an ideal but the integers are not an ideal of the real numbers. For instance, $\pi \cdot 1 = \pi \notin \mathbb{Z}$.

 # 50: Show that if m and n are distinct positive integers, then $m\mathbb{Z}$ is not ring-isomorphic to $n\mathbb{Z}$.

Let m and n be distinct positive integers. Because a ring isomorphism must take generators to generators, m would have to map to $\pm n$. Consider the case of $m \mapsto n$. Then $\phi(nn) = \phi(n + n + n + \cdots + n)$ with n copies of n. This is equal to $\phi(n) + \phi(n) + \cdots + \phi(n) = m + m + \cdots + m = nm$. But $\phi(nn) = \phi(n)\phi(n) = mm$. Since n and m are distinct, $nm \neq mm$ so there can not be any such isomorphism.

 # 66: Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \Big| a, b \in \mathbb{Z} \right\}$, and let ϕ be the mapping that takes $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ to $a - b$.

   a. **Show that ϕ is a homomorphism.**

   Addition is preserved since $\phi(\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix}) = \phi(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix}) = (a + c) - (b + d) = (a - b) + (c - d) = \phi(\begin{bmatrix} a & b \\ b & a \end{bmatrix}) + \phi(\begin{bmatrix} c & d \\ d & c \end{bmatrix})$. We can also see that multiplication is preserved since $\phi(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\begin{bmatrix} c & d \\ d & c \end{bmatrix}) = \phi(\begin{bmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{bmatrix})) = (ac + bd) - (ad + bc) = a(c - d) + b(d - c) = a(c - d) - b(c - d) = (a - b)(c - d) = \phi(\begin{bmatrix} a & b \\ b & a \end{bmatrix})\phi(\begin{bmatrix} c & d \\ d & c \end{bmatrix})$.

   b. **Determine the kernel of ϕ.**

The kernel is the set of matrixes such that $a - b = 0$, or $a = b$. Hence it is the set of matrices of the form $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$ where $a \in \mathbb{Z}$.

c. **Show that $R/Ker\ \phi$ is isomorphic to $\mathbb{Z}$.**

The image of ϕ defined as above is $\mathbb{Z}$. We know this since $\phi(R) \subseteq \mathbb{Z}$, and the matrix with $a = a$ and $b = 0$ maps to a for any $a \in \mathbb{Z}$.

d. **Is $Ker\ \phi$ a prime ideal?**

Since $\mathbb{Z}$ is an integral domain, the kernel is a prime ideal.

e. **Is $Ker\ \phi$ a maximal ideal?**

Since $\mathbb{Z}$ is not a field, the kernel is not maximal.