Homework #4 Solutions

p 286, #8 Let $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ be a ring homomorphism. Let $a = \phi(1)$. Then for any $0 \neq r \in \mathbb{Z}_n = \{1, 2, \ldots, n-1\}$ we have

$$\phi(r) = \phi(\underbrace{1 + 1 + \cdots + 1}_{r \text{ times}}) = \underbrace{\phi(1) + \phi(1) + \cdots + \phi(1)}_{r \text{ times}} = r \cdot \phi(1) = r \cdot a = ra \bmod n.$$

Since

$$a = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = a^2$$

we're finished.

p 286, #10 Let $I = \langle x^2 + 1 \rangle$ and let $f(x) \in \mathbb{Z}_3[x]$. By including zero coefficients if necessary we can write

$$f(x) = \sum_{i=0}^{n} a_{2i}x^{2i} + \sum_{j=0}^{m} a_{2j+1}x^{2j+1},$$

for some $a_i \in \mathbb{Z}_3$, i.e. we can write $f(x)$ as the sum of its even degree and odd degree terms. In $\mathbb{Z}_3[x]/I$ we have $x^2 + I = -1 + I$ so that

$$\begin{aligned}
f(x) + I &= \sum_{i=0}^{n}(a_{2i} + I)(x^{2i} + I) + \sum_{j=0}^{m}(a_{2j+1} + I)(x^{2j+1} + I) \\
&= \sum_{i=0}^{n}(a_{2i} + I)(x^2 + I)^i + \sum_{j=0}^{m}(a_{2j+1} + I)(x + I)(x^2 + I)^j \\
&= \sum_{i=0}^{n}(a_{2i} + I)(-1 + I)^i + \sum_{j=0}^{m}(a_{2j+1} + I)(x + I)(-1 + I)^j \\
&= \left(\sum_{i=0}^{n}((-1)^i a_{2i} + I)\right) + (x + I)\left(\sum_{j=0}^{m}((-1)^j a_{2j+1} + I)\right) \\
&= \left(\sum_{i=0}^{n}(-1)^i a_{2i} + x\sum_{j=0}^{m}(-1)^j a_{2j+1}\right) + I
\end{aligned}$$

or, more succinctly,

$$f(x) + I = a + bx + I$$

for some $a, b \in \mathbb{Z}_3$. Moreover, if $a + bx + I = c + dx + I$ for some $a, b, c, d \in \mathbb{Z}_3$ then $(a-c)+(b-d)x \in I$, which means that x^2+1 divides the linear polynomial $(a-c)+(b-d)x$, an obvious impossibility unless $a - c = b - d = 0$. That is, $a + bx + I = c + dx + I$ implies that $a + bx = c + dx$. Hence, every element in $\mathbb{Z}_3[x]/I$ can be expressed *uniquely* in the form $a + bx + I$, $a, b \in \mathbb{Z}_3$. We will use this fact below.

Now define $\phi : \mathbb{Z}_3[i] \to \mathbb{Z}_3[x]/I$ by $\phi(a+bi) = a + bx + I$. This is a homomorphism since for any $a, b, c, d \in \mathbb{Z}_3$ we have

$$\begin{aligned}
\phi((a+bi)(c+di)) &= \phi((ac-bd)+(ad+bc)i) \\
&= (ac-bd)+(ad+bc)x+I \\
&= (a+bx+I)(c+dx+I)-(bd+I)(x^2+1+I) \\
&= (a+bx+I)(c+dx+I) \\
&= \phi(a+bi)\phi(c+di)
\end{aligned}$$

and

$$\begin{aligned}
\phi((a+bi)+(c+di)) &= \phi((a+c)+(b+d)i) \\
&= (a+c)+(b+d)x+I \\
&= (a+bx)+(c+dx)+I \\
&= (a+bx+I)+(c+dx+I) \\
&= \phi(a+bi)+\phi(c+di).
\end{aligned}$$

Moreover, the result of the preceding paragraph implies that this function is one-to-one and onto, hence provides an isomorphism between $\mathbb{Z}_3[i]$ and $\mathbb{Z}_3[x]/I$.

p 286, #12 Define $\phi : \mathbb{Z}[\sqrt{2}] \to H$ by

$$\phi(a+bi) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

This is obviously one-to-one and onto so to prove it is an isomorphism it suffices to show that it preserves addition and multiplication. Addition is easy: for any $a, b, c, d \in \mathbb{Z}$

$$\begin{aligned}
\phi((a+b\sqrt{2})+(c+d\sqrt{2})) &= \phi((a+c)+(b+d)i) = \begin{pmatrix} a+c & 2(b+d) \\ b+d & a+c \end{pmatrix} \\
&= \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} = \phi(a+b\sqrt{2})+\phi(c+d\sqrt{2}).
\end{aligned}$$

Multiplication is no more difficult, just more interesting: for $a, b, c, d \in \mathbb{Z}$ we have

$$\begin{aligned}
\phi((a+b\sqrt{2})(c+d\sqrt{2})) &= \phi((ac+2bd)+(ad+bc)\sqrt{2}) = \begin{pmatrix} ac+2bd & 2(ad+bc) \\ ad+bc & ac+2bd \end{pmatrix} \\
&= \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} c & 2d \\ d & c \end{pmatrix} = \phi(a+bi)\phi(c+di)
\end{aligned}$$

and we're finished!

p 287, #18 Let $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ be an isomorphism of rings. According to exercise 8 there is an $a \in \mathbb{Z}_n$ satisfying $a^2 = a$ so that $\phi(x) = ax$ for all $x \in \mathbb{Z}_n$. In order for ϕ to be an isomorphism we must also have $a = a \cdot 1 = \phi(1) = 1$. Therefore $\phi(x) = x$ for all x, i.e. ϕ must be the identity homomorphism.

p 287, #24 Let $\phi : R \to S$ be a homomorphism of rings and let $a \in R$ be an idempotent. Then

$$\phi(a)^2 = \phi(a^2) = \phi(a)$$

since $a^2 = a$. Hence, $\phi(a)$ is an idempotent as well.

p 288, #36 Let $\phi : \mathbb{Q} \to \mathbb{Q}$ be an homomorphism of rings. Since $\mathbb{Q}$ is a field and $\ker \phi$ is an ideal, we must have $\ker \phi = \{0\}$ or $\ker \phi = \mathbb{Q}$. That is, either ϕ is one-to-one or ϕ maps every element to 0. Clearly there is no more work to be done in the latter case, so we assume ϕ is one-to-one. The only idempotents in a domain are 0 and 1 so the previous exercise implies that $\phi(1)$ is 0 or 1. But $\phi(0) = 0$ and ϕ is one-to-one, so $\phi(1) = 1$. It follows that for any positive integer n we have

$$\phi(n) = \phi(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\phi(1) + \phi(1) + \cdots + \phi(1)}_{n \text{ times}} = n.$$

Moreover, $1 = \phi(1) = \phi((-1)^2) = \phi(-1)^2$ implies $\phi(-1) = \pm 1$, so one-to-one-ness give $\phi(-1) = -1$. Hence, if n is a negative integer, $n = -m$ with $m > 0$ and

$$\phi(n) = \phi(-1 \cdot m) = \phi(-1)\phi(m) = -1 \cdot m = n.$$

Therefore $\phi(n) = n$ for all $n \in \mathbb{Z}$. If n is a nonzero integer then we also have

$$1 = \phi(1) = \phi\left(n \cdot \frac{1}{n}\right) = \phi(n)\phi\left(\frac{1}{n}\right) = n\phi\left(\frac{1}{n}\right)$$

from which it follows that $\phi(1/n) = 1/n$. Finally, for any $r \in \mathbb{Q}$ we can write $r = a/b$ with $a, b \in \mathbb{Z}$, $b \neq 0$ so that

$$\phi(r) = \phi\left(\frac{a}{b}\right) = \phi\left(a \cdot \frac{1}{b}\right) = \phi(a)\phi\left(\frac{1}{b}\right) = a \cdot \frac{1}{b} = \frac{a}{b} = r.$$

Thus, if ϕ is a one-to-one homomorphism from $\mathbb{Q}$ to $\mathbb{Q}$ then ϕ is the identity map.

p 288, #38 We will need the following elementary lemma.

Lemma 1. *Let p be a prime. Then the binomial coefficient $\binom{p}{k}$ is divisible by p for all $1 \leq k \leq p - 1$.*

Proof. We know

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{p(p-1)!}{(p-k)!k!}$$

so that p divides $(p-k)!k!\binom{p}{k}$. Since p is prime this means that p must divide one of $2, 3, \ldots, p-k$ or $2, 3, \ldots, k$ or $\binom{p}{k}$. Since both k and $p-k$ are strictly less than p the only possibility is the last, i.e. p must divide $\binom{p}{k}$. □

We now complete the exercise. Let R be a commutative ring with prime characteristic p and define $\phi : R \to R$ by $\phi(x) = x^p$. For any $x, y \in R$ we have

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$$

and

$$\phi(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = \phi(x) + \phi(y).$$

The middle terms in the last expression vanish because, according to the lemma, all the binomial coefficients are divisible by p, the characteristic of R. Hence, ϕ is a homomorphism. This homomorphism figures prominently in the Galois theory of finite fields.

p 288, #40 Let F be a field, R be a ring and $\phi : F \to R$ be an onto homomorphism. According to the first isomorphism theorem $F/\ker\phi \cong R$. If R has more than one element then we cannot have $\ker\phi = F$. However, since the kernel is an ideal and F is a field, the only other option we have is $\ker\phi = \{0\}$. Hence, ϕ is also one-to-one and is therefore an isomorphism.

p 288, #46 Let $\phi : \mathbb{R} \to \mathbb{R}$ be an isomorphism of rings. We can argue exactly as in Exercise 36 to conclude that $\phi(r) = r$ for all $r \in \mathbb{Q}$.[1] Let $x, y \in \mathbb{R}$ with $x < y$. Then $y - x > 0$ so there is a $z \in \mathbb{R}^+$ so that $x - y = z^2$. Then

$$\phi(y) - \phi(x) = \phi(y - x) = \phi(z^2) = \phi(z)^2 > 0$$

since $\phi(z) \neq 0$ as ϕ is one-to-one. That is, if $x < y$ then $\phi(x) < \phi(y)$, i.e. ϕ preserves the natural order on $\mathbb{R}$. Let $x \in \mathbb{R}$ and suppose that $x < \phi(x)$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$ we can find an $r \in \mathbb{Q}$ with $x < r < \phi(x)$. But then $\phi(x) < \phi(r) = r < \phi(x)$, an impossibility. We have a similar contradiction if $x > \phi(x)$ and so we conclude that $\phi(x) = x$. Since x was an arbitrary element of $\mathbb{R}$ we conclude that ϕ is the identity map.

p 289, #60 a. Let $\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} c & d \\ d & c \end{pmatrix} \in R$. Then

$$\begin{aligned} \phi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} + \begin{pmatrix} c & d \\ d & c \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix}\right) = (a+c) - (b+d) \\ &= (a-b) + (c-d) = \phi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) + \phi\left(\begin{pmatrix} c & d \\ d & c \end{pmatrix}\right) \end{aligned}$$

and

$$\begin{aligned} \phi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\begin{pmatrix} c & d \\ d & c \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{pmatrix}\right) = (ac+bd) - (ad+bc) \\ &= (a-b)(c-d) = \phi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right)\phi\left(\begin{pmatrix} c & d \\ d & c \end{pmatrix}\right) \end{aligned}$$

proving that ϕ is a homomorphism.

[1] We have seen that any field of characteristic 0 contains $\mathbb{Q}$ as a subfield and that any field of characteristic p contains $\mathbb{Z}_p$ as a subfield. In each case, these fields are called the *prime subfields* and it is a general fact that any automorphism of a field must fix its prime subfield element-wise.

b. $\begin{pmatrix} a & b \\ b & a \end{pmatrix} \in R$ is in the kernel of ϕ if and only if $a - b = 0$ or $a = b$. Thus

$$\ker \phi = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| \, a \in \mathbb{Z} \right\}.$$

c. Since $\phi : R \to \mathbb{Z}$ is a homomorphism and is clearly onto, the first isomorphism theorem tells us that $R/\ker\phi \cong \mathbb{Z}$.

d. Since R is a commutative ring with identity and $R/\ker\phi \cong \mathbb{Z}$ is an integral domain, we can apply Theorem 14.3 to conclude that $\ker\phi$ is indeed a prime ideal.

e. Since R is a commutative ring with identity and $R/\ker\phi \cong \mathbb{Z}$ is not a field, we can apply Theorem 14.4 to conclude that $\ker\phi$ is not a maximal ideal.