15 Chapter

Definition 15.1. *Ring Homomorphism, Ring Isomorphism*
A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R,

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism that is both one-to-one and onto is called a ring isomorphism.

Theorem 15.1. *Properties of Ring Homomorphisms*
Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.

1. *For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.*
2. *$\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S.*
3. *If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.*
4. *$\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.*
5. *If R is commutative, then $\phi(R)$ is commutative.*
6. *If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.*
7. *ϕ is an isomorphism if and only if ϕ is onto and $Ker\,\phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.*
8. *If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.*

Theorem 15.2. *Kernels Are Ideals*
Let ϕ be a ring homomorphism from a ring R to a ring S. Then $Ker\,\phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

Theorem 15.3. *First Isomorphism Theorem for Rings*
Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/Ker\,\phi$ to $\phi(R)$, given by $r + Ker\,\phi \to \phi(r)$, is an isomorphism. In symbols, $R/Ker\,\phi \approx \phi(R)$.

Theorem 15.4. *Ideals Are Kernels*
Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \to r + A$ from R to R/A.

Theorem 15.5. *Homomorphism from $\mathbb{Z}$ to a Ring with Unity*
Let R be a ring with unity 1. The mapping $\phi : \mathbb{Z} \to R$ given by $n \to n \cdot 1$ is a ring homomorphism.

Corollary 15.6. *A Ring with Unity Contains $\mathbb{Z}_n$ or $\mathbb{Z}$*
If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 15.7. *$\mathbb{Z}_m$ Is a Homomorphic Image of $\mathbb{Z}$*
For any positive integer m, the mapping of $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \to x \mod m$ is a ring homomorphism.

Corollary 15.8. *A Field Contains $\mathbb{Z}_p$ or $\mathbb{Q}$ (Steinitz, 1910)*
If F is a field of characteristic p, then F contains a subfield isomorphic to $\mathbb{Z}_p$. If F is a field of characteristic 0, then F contains a subfield isomorphic to the rational numbers.

Theorem 15.9. *Field of Quotients*
Let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D.

Exercises

3.1 Prove Theorem 15.3.

We're asked to prove the *First Isomorphism Theorem for Rings*, or that $r + \operatorname{Ker}\phi \to \phi(r)$ is an isomorphism. Due to the fact that ϕ is a ring homomorphism from R to S, we know that for $a, b \in R$ and $\phi(a), \phi(b) \in S$ that $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. We also know from Theorem 15.1.7 that ϕ is an isomorphism if and only if ϕ is onto and $\operatorname{Ker}\phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$. We also know from 15.2 that $\operatorname{Ker}\phi$ is an ideal of R.

I'm going to try and use the notation $0_S, 1_S$ for the additive and multiplicative identities of S, respectively.

Intuitively, it's clear that $\operatorname{Ker}\phi = \{0\}$, or $\phi(r + \operatorname{Ker}\phi) = \phi(r) + \phi(\operatorname{Ker}\phi) = \phi(r) + \phi(\{0\}) = \phi(r) + \phi(0)$. However, we know that the additive identity of R, 0, must be mapped to the additive identity of S; this means that $\phi(r) + \phi(0) = \phi(r) + 0_S = \phi(r)$.

On the other hand, let's assume that there is an element $a \in \operatorname{Ker}\phi$ such that $a \neq 0$. This means that we would have the expression $\phi^{-1}(r) + \phi^{-1}(a) = r + \operatorname{Ker}\phi + a + \operatorname{Ker}\phi = r + a + \operatorname{Ker}\phi$ or that $\phi^{-1}(r + a) = r + a + \operatorname{Ker}\phi$. Although since $a \neq 0$ we can assume that $\operatorname{Ker}\phi$ possesses at least 0 and a, or $a + \operatorname{Ker}\phi$ is at least $\{a, a + a\}$; which we can then evaluate $\phi(r) + \phi(\{a, a + a\})$ as $phi(r) + \phi(a), \phi(r) + \phi(a + a)$. But $a \in \operatorname{Ker}\phi$ which implies that $\phi(r) + \phi(a), \phi(r) + \phi(a + a) = \phi(r)$. I know I've made an error in here somewhere but I can't find where.

3.2 Prove Theorem 15.1.6
If R has a unity 1, $S \neq \{0\}$ and ϕ is onto, then $\phi(1)$ is the unity of S.

We assume that R has a unity 1, and we know that ϕ is a homomorphism from R to S.Now let a be an element of R. So $\phi(1a) = \phi(1)\phi(a)$, but $\phi(1a) = \phi(a)$; which implies that $\phi(1)\phi(a) = \phi(a)$, due to the fact that ϕ is onto. This immediately implies that $\phi(1)$ is the unity of S by the definition of unity.

13. Let

$$S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$$

Show that $\phi : \mathbb{C} \to S$ given by

$$\phi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

is a ring isomorphism.

Restatement: Show $\phi(a_0 + b_0 i + a_1 + b_1 i) = \phi(a_0 + b_0 i) + \phi(a_1 + b_1 i)$ and $\phi((a_0 + b_0 i)(a_1 + b_1 i)) = \phi(a_0 + b_0 i)\phi(a_1 + b_1 i)$.

(a) $\phi(a_0 + b_0 i + a_1 + b_1 i) = \phi(a_0 + a_1 + (b_0 + b_1)i) = \begin{bmatrix} a_0 + a_1 & b_0 + b_1 \\ -(b_0 + b_1) & a_0 + a_1 \end{bmatrix}$.
Which we can then see $\begin{bmatrix} a_0 + a_1 & b_0 + b_1 \\ -(b_0 + b_1) & a_0 + a_1 \end{bmatrix} = \begin{bmatrix} a_0 & b_0 \\ -b_0 & a_0 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix}$, by the laws of matrix addition.
Observing the right hand side, we see $\phi(a_0 + b_0 i) + \phi(a_1 + b_1 i) = \begin{bmatrix} a_0 & b_0 \\ -b_0 & a_0 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix}$. This implies that $\phi(a_0 + b_0 i + a_1 + b_1 i) = \phi(a_0 + b_0 i) + \phi(a_1 + b_1 i)$.

(b) $\phi(a_0+b_0i)\phi(a_1+b_1i) = \begin{bmatrix} a_0 & b_0 \\ -b_0 & a_0 \end{bmatrix}\begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} = \begin{bmatrix} a_0\,a_1 - b_0\,b_1 & a_0\,b_1 + b_0\,a_1 \\ -a_0\,b_1 - b_0\,a_1 & a_0\,a_1 - b_0\,b_1 \end{bmatrix}$.

Now, by looking to the left hand side, we observe

$$\phi((a_0+b_0i)(a_1+b_1i)) = \phi(a_0\,a_1 - b_0\,b_1 + (a_0\,b_1 + b_0\,a_1)\,i).$$

Which evaluates as $\begin{bmatrix} a_0\,a_1 - b_0\,b_1 & a_0\,b_1 + b_0\,a_1 \\ -(a_0\,b_1 + b_0\,a_1) & a_0\,a_1 - b_0\,b_1 \end{bmatrix}$, and means that $\phi((a_0+b_0i)(a_1+b_1i)) = \phi(a_0+b_0i)\phi(a_1+b_1i)$.

14. Let $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \;\middle|\; a,b \in \mathbb{Z} \right\}.$$

Show that $\mathbb{Z}[\sqrt{2}]$ and H are isomorphic as rings.

Let ϕ be a homomorphism from $\mathbb{Z}[\sqrt{2}]$ to H, where $\phi(a+b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. Show that $\operatorname{Ker}\phi = \{0\}$.

Define $A = \begin{bmatrix} a_0 & 2b_0 \\ b_0 & a_0 \end{bmatrix}$ and $B = \begin{bmatrix} a_1 & 2b_1 \\ b_1 & a_1 \end{bmatrix}$. This implies that $\phi^{-1}(A) = a_0 + b_0\sqrt{2}$ and $\phi^{-1}(B) = a_1 + b_1\sqrt{2}$.

So we begin with $\phi^{-1}(A\times B) = \phi^{-1}(\begin{bmatrix} a_0a_1 + 2b_0b_1 & 2a_1b_0 + 2a_0b_1 \\ a_1b_0 + a_0b_1 & a_0a_1 + 2b_0b_1 \end{bmatrix}) = a_0a_1 + 2b_0b_1 + (a_1b_0 + a_0b_1)\sqrt{2}$, which is not equal to zero unless either A or B is equal to the zero matrix; due to the fact that $\mathbb{Z}$ is an integral domain.

We can say the same of $\phi^{-1}(\begin{bmatrix} a_0 + a_1 & 2b_0 + 2b_1 \\ b_0 + b_1 & a_0 + a_1 \end{bmatrix}) = a_0 + a_1 + (b_0 + b_1)\sqrt{2}$, which is only equal to 0 if A is the additive inverse of B or vice versa, as this would imply that we started with the zero matrix.

This shows that $\operatorname{Ker}\phi = \{0\}$, and that ϕ is an isomorphism.

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

Let $A_0 = \begin{bmatrix} a_0 & b_0 \\ 0 & c_0 \end{bmatrix}$, $A_1 = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$, and $\phi : \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mapsto a$.We can determine

$$\phi(A_0 + A_1) = \phi(\begin{bmatrix} a_0 & b_0 \\ 0 & c_0 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}) = \phi(\begin{bmatrix} a_0 + a_1 & b_0 + b_1 \\ 0 & c_0 + c_1 \end{bmatrix}) = a_0 + a_1.$$

Or,

$$\phi(A_0) + \phi(A_1) = a_0 + a_1$$

.

Under multiplication,

$$\phi(A_0 \times A_1) = \phi(\begin{bmatrix} a_0a_1 & a_0b_1 + b_0c_1 \\ 0 & c_0c_1 \end{bmatrix}) = a_0a_1,$$

or,

$$\phi(A_0) \times \phi(A_1) = a_0a_1$$

Which shows that ϕ is a homomorphism.

22. Determine all ring isomorphisms from $\mathbb{Z}_n$ to itself.

This one has me a bit baffled. If n is prime, then there should be n isomorphisms, since every element is a unit. However, if n is not prime, then we don't have an integral domain. Assuming our mapping is defined as $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$, $\operatorname{Ker}\phi \neq \{0\}$.

27. Let R be a ring with unity and let ϕ be a ring homomorphism from R onto S where S has more than one element. Prove that S has a unity.

Let 1 be the unity of R. Because R has unity and S has more than one element, or $S \neq \{0\}$, we only need to show that ϕ is onto. We know that R has an additive identity, 0, which we claim is mapped to 0_S. Now, consider two elements in S, $\phi(a)$ and $\phi(b)$. Because ϕ is a homomorphism we know that $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. Allowing a to be 1, we see that $\phi(a)\phi(b) = \phi(1)\phi(b) = \phi(1b) = \phi(b)$, which implies that $\phi(1)$ is the unity of S.

37. For any integer $n > 1$, prove that $\mathbb{Z}_n[x]/\langle x\rangle$ is isomorphic to $\mathbb{Z}_n$.

Let $P(x), Q(x) \in \mathbb{Z}_n[x]$, we can see that $\mathbb{Z}_n[x]/\langle x\rangle$ is of the form $P(x) + \langle x\rangle \mod n$. Show that the mapping $\phi : P(x) + \langle x\rangle \mod n \mapsto c$ where $c \in \mathbb{Z}_n$, and c is the constant term of $P(x)$. It makes sense to suppose that if $P(x)$ is the zero polynomial, $P(x) + \langle x\rangle \to 0$, as everything in $\langle x\rangle$ is of the form $xQ(x)$. So we have $P(x) + xQ(x) \mod n$, which under our mapping only preserves c. Now, as a result of everything in $\langle x\rangle$ being of the form $xQ(x)$, we know that every $P(x)$ with zero constants must be contained in $\langle x\rangle$, which implies that $\operatorname{Ker}\phi = \{0\}$, and ϕ is an isomorphism.

38. For any integer $n > 1$, prove that $\langle x\rangle$ is a maximal ideal of $\mathbb{Z}_n[x]$ if and only if n is prime.

Let $Q(x) \in \mathbb{Z}_n[x]$. Everything in $\langle x\rangle$ looks like $xQ(x) \mod n$. Now, as we showed above $\mathbb{Z}_n/\langle x\rangle$, is isomorphic to $\mathbb{Z}_n$, which in this scenario implies that $\mathbb{Z}_n/\langle x\rangle$ is isomorphic to a field. By Theorem 14.4, we know that $\mathbb{Z}_n/\langle x\rangle$ is a field if and only if $\langle x\rangle$ is maximal. We just showed that $\mathbb{Z}_n/\langle x\rangle$ is a field, which means $\langle x\rangle$ is maximal.

42. Determine all ring homomorphisms from $\mathbb{Q}$ to $\mathbb{Q}$.

44. Let R be a commutative ring of prime characteristic p. Show that the *Frobenius* map $x \mapsto x^p$ is a ring homomorphism from R to R.

Let $x, y \in R$, and define the Frobenius map as $f : R \to R$.

(a) Show that $f(x+y) = f(x) + f(y)$. We see that $f(x+y) = (x+y)^p = \underbrace{(x+y)(x+y)\dots(x+y)}_{p \text{ times}}$

By the Binomial Theorem, we know that

$$(x+y)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1} + \binom{p}{p}y^p$$

So now, by observing that $0 < k < p$ in $\binom{p}{k}$, we can reduce the expression to $\binom{p}{k} = \frac{p!}{(p-k)!k!}$, which always has a factor of p. Thus, utilizing the fact that R has characteristic p, we see that

$$\begin{aligned}(\mathrm{x+y})^p &= \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1} + \binom{p}{p}y^p \\ &= \binom{p}{0}\mathrm{x}^p + p\cdot\left(\binom{p-1}{1}x^{p-1}y + \cdots + \binom{p-1}{p-1}xy^{p-1}\right) + \binom{p}{p}y^p \\ &= \mathrm{x}^p + 0 + y^p \\ &= \mathrm{x}^p + y^p\end{aligned}$$

Almost trivially at this point, $f(x) + f(y) = x^p + y^p$.

This means that $f(x+y) = f(x) + f(y)$.

1. Show that $f(xy) = f(x)f(y)$. So the expression

$$f(xy) = (xy)^p = \underbrace{(xy)(xy)\dots(xy)}_{p \text{ times}} = \overbrace{\underbrace{(xx\dots)}_{p \text{ times}}\underbrace{(yy\dots)}_{p \text{ times}}}^{\text{by the fact that } R \text{ is commutative}} = 0 \cdot 0 = 0,$$

or $f(x)f(y) = x^p y^p = \underbrace{(x)(x)\dots}_{p \text{ times}}\underbrace{(y)(y)\dots}_{p \text{ times}} = 0 \cdot 0 = 0$, which implies that $f(xy) = f(x)f(y)$.

This implies that f is a homomorphism from R to R.

Let $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ and $\mathbb{Q}[\sqrt{5}] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\right\}$. Show that these two rings are not ring-isomorphic.

A mapping $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$, defined as $\phi : a+b\sqrt{2} \mapsto a+b\sqrt{5}$ is not onto. Take $a_0+b_0\sqrt{5}, a_1+b_1\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$, $\phi^{-1}((a_0+b_0\sqrt{5})(a_1+b_1\sqrt{5})) = \phi^{-1}(a_0a_1+5b_0b_1+(a_1b_0+a_0b_1)\sqrt{5}) = a_0a_1+5b_0b_1+(a_1b_0+a_0b_1)\sqrt{2}$, but $\phi^{-1}(a_0 + b_0\sqrt{5})\phi^{-1}((a_1 + b_1\sqrt{5})) = (a_0 + b_0\sqrt{2})(a_1 + b_1\sqrt{2}) = a_0a_1 + 2b_0b_1 + (a_1b_0 + a_0b_1)\sqrt{2}$

Which shows that $\mathbb{Q}[\sqrt{2}]$ is not isomorphic to $\mathbb{Q}[\sqrt{5}]$.