Introduction to Modern Algebra

Part V. Ideals and Factor Rings

V.26 Homomorphisms and Factor Rings

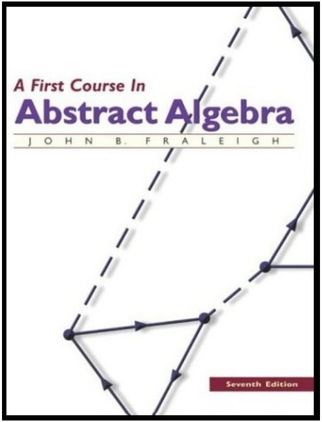

Table of contents

Theorem 26.3

Theorem 26.3 (Analogue of Theorem 13.12). Let φ be a homomorphism of a ring R into a ring R'. If 0 is the additive identity in R, then $\varphi(0) = 0'$ is the additive identity in R', and if $a \in R$, then $\varphi(-a) = -\varphi(a)$. If S is a subring of R, then $\varphi[S]$ is a subring of R'. If S' is a subring of R', then $\varphi^{-1}[S']$ is a subring of R. If R has unity 1, then $\varphi(1)$ is unity for $\varphi[R]$.

Proof. We can consider φ as a homomorphism from group $\langle R, +\rangle$ to group $\langle R', +'\rangle$ and so by Theorem 13.12, $\varphi(0) = 0'$ and $\varphi(-a) = -\varphi(a)$, as claimed.

Theorem 26.3

Theorem 26.3 (Analogue of Theorem 13.12). Let φ be a homomorphism of a ring R into a ring R'. If 0 is the additive identity in R, then $\varphi(0) = 0'$ is the additive identity in R', and if $a \in R$, then $\varphi(-a) = -\varphi(a)$. If S is a subring of R, then $\varphi[S]$ is a subring of R'. If S' is a subring of R', then $\varphi^{-1}[S']$ is a subring of R. If R has unity 1, then $\varphi(1)$ is unity for $\varphi[R]$.

Proof. We can consider φ as a homomorphism from group $\langle R, +\rangle$ to group $\langle R', +'\rangle$ and so by Theorem 13.12, $\varphi(0) = 0'$ and $\varphi(-a) = -\varphi(a)$, as claimed.

Again, by Theorem 13.12, if S is a subring of R, then $\langle \varphi[S], +'\rangle$ is an abelian subgroup of $\langle R', +'\rangle$, so we only need check multiplication. If $\varphi(S_1), \varphi(S_2) \in \varphi[S]$, then $\varphi(S_1)\varphi(S_2) = \varphi(S_1 S_2)$ and $\varphi(S_1 S_2) \in \varphi[S]$, so $\varphi(S_1)\varphi(S_2) \in \varphi[S]$ and $\varphi[S]$ is closed under multiplication. So $\varphi[S]$ is a subring of R' (associativity of multiplication and the distribution laws are inherited from R'), as claimed.

Theorem 26.3

Theorem 26.3 (Analogue of Theorem 13.12). Let φ be a homomorphism of a ring R into a ring R'. If 0 is the additive identity in R, then $\varphi(0) = 0'$ is the additive identity in R', and if $a \in R$, then $\varphi(-a) = -\varphi(a)$. If S is a subring of R, then $\varphi[S]$ is a subring of R'. If S' is a subring of R', then $\varphi^{-1}[S']$ is a subring of R. If R has unity 1, then $\varphi(1)$ is unity for $\varphi[R]$.

Proof. We can consider φ as a homomorphism from group $\langle R, +\rangle$ to group $\langle R', +'\rangle$ and so by Theorem 13.12, $\varphi(0) = 0'$ and $\varphi(-a) = -\varphi(a)$, as claimed.

Again, by Theorem 13.12, if S is a subring of R, then $\langle \varphi[S], +'\rangle$ is an abelian subgroup of $\langle R', +'\rangle$, so we only need check multiplication. If $\varphi(S_1), \varphi(S_2) \in \varphi[S]$, then $\varphi(S_1)\varphi(S_2) = \varphi(S_1 S_2)$ and $\varphi(S_1 S_2) \in \varphi[S]$, so $\varphi(S_1)\varphi(S_2) \in \varphi[S]$ and $\varphi[S]$ is closed under multiplication. So $\varphi[S]$ is a subring of R' (associativity of multiplication and the distribution laws are inherited from R'), as claimed.

Theorem 26.3 (continued)

Theorem 26.3 (Analogue of Theorem 13.12). Let φ be a homomorphism of a ring R into a ring R'. If 0 is the additive identity in R, then $\varphi(0) = 0'$ is the additive identity in R', and if $a \in R$, then $\varphi(-a) = -\varphi(a)$. If S is a subring of R, then $\varphi[S]$ is a subring of R'. If S' is a subring of R', then $\varphi^{-1}[S']$ is a subring of R. If R has unity 1, then $\varphi(1)$ is unity for $\varphi[R]$.

Proof. Theorem 13.12 also shows that if S' is a subring of R', then $\langle \varphi^{-1}[S], + \rangle$ is an abelian subgroup of $\langle R, + \rangle$. Let $a, b \in \varphi^{-1}[S']$ is closed under multiplication. So $\varphi^{-1}[S']$ is a subring of R (assoicativity of multiplication and the distribution laws are inherited form R), as claimed.

Finally, if R has unity 1, then for all $r \in R$, $\varphi(r) = \varphi(1r) = \varphi(r1) = \varphi(1)\varphi(r) = \varphi(r)\varphi(1)$ and so $\varphi(1)$ is unity for $\varphi[R]$, as claimed. □

Theorem 26.3 (continued)

Theorem 26.3 (Analogue of Theorem 13.12). Let φ be a homomorphism of a ring R into a ring R'. If 0 is the additive identity in R, then $\varphi(0) = 0'$ is the additive identity in R', and if $a \in R$, then $\varphi(-a) = -\varphi(a)$. If S is a subring of R, then $\varphi[S]$ is a subring of R'. If S' is a subring of R', then $\varphi^{-1}[S']$ is a subring of R. If R has unity 1, then $\varphi(1)$ is unity for $\varphi[R]$.

Proof. Theorem 13.12 also shows that if S' is a subring of R', then $\langle \varphi^{-1}[S], + \rangle$ is an abelian subgroup of $\langle R, + \rangle$. Let $a, b \in \varphi^{-1}[S']$ is closed under multiplication. So $\varphi^{-1}[S']$ is a subring of R (assoicativity of multiplication and the distribution laws are inherited form R), as claimed.

Finally, if R has unity 1, then for all $r \in R$, $\varphi(r) = \varphi(1r) = \varphi(r1) = \varphi(1)\varphi(r) = \varphi(r)\varphi(1)$ and so $\varphi(1)$ is unity for $\varphi[R]$, as claimed. □

Theorem 26.5

Theorem 26.5 (Analogue of Theorem 13.15). Let $\varphi : R \to R'$ be a ring homomorphism and let $H = \text{Ker}(\varphi)$. Let $a \in R$. Then $\varphi^{-1}[\varphi(a)] = a + H = H + a$, where $a + H = H + a$ is the coset containing a of the commutative additive group $\langle H, + \rangle$.

Proof. This follows immediately from Theorem 13.15 since $\langle R, + \rangle$ is an abelian group and φ restricted to $\langle R, + \rangle$ is a group homomorphism. □

Theorem 26.5

Theorem 26.5 (Analogue of Theorem 13.15). Let $\varphi : R \to R'$ be a ring homomorphism and let $H = \text{Ker}(\varphi)$. Let $a \in R$. Then $\varphi^{-1}[\varphi(a)] = a + H = H + a$, where $a + H = H + a$ is the coset containing a of the commutative additive group $\langle H, +\rangle$.

Proof. This follows immediately from Theorem 13.15 since $\langle R, +\rangle$ is an abelian group and φ restricted to $\langle R, +\rangle$ is a group homomorphism. □

Corollary 26.6

Corollary 26.6 (Analogue of Corollary 13.18). A ring homomorphism $\varphi : R \to R'$ is a one-to-one map if and only if $\text{Ker}\,(\varphi) = \{0\}$.

Proof. This follows immediately from Corollary 13.18, as in the proof of Theorem 26.5. □

Corollary 26.6

Corollary 26.6 (Analogue of Corollary 13.18). A ring homomorphism $\varphi : R \to R'$ is a one-to-one map if and only if $\text{Ker}(\varphi) = \{0\}$.

Proof. This follows immediately from Corollary 13.18, as in the proof of Theorem 26.5. □

Theorem 26.7

Theorem 26.7 (Analogue of Theorem 14.1). Let $\varphi : R \to R'$ be a ring homomorphism with kernel H. Then the additive cosets of H form a ring R/H whose binary operations are defined by choosing representatives. That is, the sum of two cosets is defined by $(a+H)+(b+H)=(a+b)+H$ and the product of the cosets is defined by $(a+H)(b+H)=(ab)+H$. Also, the map $\mu : R/H \to \varphi[R]$ defined by $\mu(a+H)=\varphi(a)$ is an isomorphism.

Proof. The additive parts of the theorem follow from Theorem 14.1 (R_1) and we must only check the multiplicative parts.

Theorem 26.7

Theorem 26.7 (Analogue of Theorem 14.1). Let $\varphi : R \to R'$ be a ring homomorphism with kernel H. Then the additive cosets of H form a ring R/H whose binary operations are defined by choosing representatives. That is, the sum of two cosets is defined by $(a+H)+(b+H)=(a+b)+H$ and the product of the cosets is defined by $(a+H)(b+H)=(ab)+H$. Also, the map $\mu : R/H \to \varphi[R]$ defined by $\mu(a+H)=\varphi(a)$ is an isomorphism.

Proof. The additive parts of the theorem follow from Theorem 14.1 (R_1) and we must only check the multiplicative parts.

First to show that multiplication of cosets in terms of representatives is well defined. Let $h_1, h_2 \in H$ and consider the representatives $a+h_1 \in a+H$ and $b+h_2 \in b+H$. Let $c=(a+h_1)(b+h_2)=ab+ah_2+h_1b+h_1h_2$. We now show $c \in ab+H=\varphi^{-1}[\varphi(ab)]$ by showing $\varphi(c)=\varphi(ab)$.

Theorem 26.7

Theorem 26.7 (Analogue of Theorem 14.1). Let $\varphi : R \to R'$ be a ring homomorphism with kernel H. Then the additive cosets of H form a ring R/H whose binary operations are defined by choosing representatives. That is, the sum of two cosets is defined by $(a+H)+(b+H)=(a+b)+H$ and the product of the cosets is defined by $(a+H)(b+H)=(ab)+H$. Also, the map $\mu : R/H \to \varphi[R]$ defined by $\mu(a+H)=\varphi(a)$ is an isomorphism.

Proof. The additive parts of the theorem follow from Theorem 14.1 (R_1) and we must only check the multiplicative parts.

First to show that multiplication of cosets in terms of representatives is well defined. Let $h_1, h_2 \in H$ and consider the representatives $a+h_1 \in a+H$ and $b+h_2 \in b+H$. Let $c=(a+h_1)(b+h_2)=ab+ah_2+h_1b+h_1h_2$. We now show $c \in ab+H=\varphi^{-1}[\varphi(ab)]$ by showing $\varphi(c)=\varphi(ab)$.

Theorem 26.7 (continued 1)

Proof (continued). We have

$$\begin{aligned}
\varphi(c) &= \varphi(ab + ah_2 + h_1 b + h_1 h_2) \\
&= \varphi(ab) + \varphi(ah_2) + \varphi(h_1 b) + \varphi(h_1 h_2) \\
&= \varphi(ab) + \varphi(a)\varphi(h_2) + \varphi(h_1)\varphi(b) + \varphi(h_1)\varphi(h_2) \\
&= \varphi(ab) + \varphi(a)0' + 0'\varphi(c) + 0'0' \text{ since } \mathrm{Ker}(\varphi) = H \\
&= \varphi(ab) + 0' + 0' + 0' = \varphi(ab).
\end{aligned}$$

So multiplication is independent of coset representatives and coset multiplications is well defined.

Let $a + H, b + H, c + H \in R/H$. Then

$$((a+H)(b+H))(c+H) = (ab+H)(c+H) = (ab)c + H = a(bc) + H$$

$$= (a+H)(bc+H) = (a+H)((b+H)(c+H))$$

and so coset multiplication is associative (R_2).

Theorem 26.7 (continued 1)

Proof (continued). We have

$$\begin{aligned}\varphi(c) &= \varphi(ab + ah_2 + h_1 b + h_1 h_2) \\ &= \varphi(ab) + \varphi(ah_2) + \varphi(h_1 b) + \varphi(h_1 h_2) \\ &= \varphi(ab) + \varphi(a)\varphi(h_2) + \varphi(h_1)\varphi(b) + \varphi(h_1)\varphi(h_2) \\ &= \varphi(ab) + \varphi(a)0' + 0'\varphi(c) + 0'0' \text{ since } \mathrm{Ker}(\varphi) = H \\ &= \varphi(ab) + 0' + 0' + 0' = \varphi(ab).\end{aligned}$$

So multiplication is independent of coset representatives and coset multiplications is well defined.

Let $a + H, b + H, c + H \in R/H$. Then

$$((a+H)(b+H))(c+H) = (ab+H)(c+H) = (ab)c + H = a(bc) + H$$

$$= (a+H)(bc+H) = (a+H)((b+H)(c+H))$$

and so coset multiplication is associative (R_2).

Theorem 26.7 (continued 2)

Proof (continued). Next,

$$(a+H)((b+H)(c+H)) = (a+H)(b+c+H) = a(b+c)+H$$

$$= ab+ac+H = (ab+H)+(ac+H) = (a+H)(b+H)+(a+H)(c+H)$$

and left distribution holds, with right distribution follows similarly (R_3). Hence, R/H is a ring, as claimed.

Theorem 14.1 shows that the map μ defined in the theorem is well-defined, one-to-one, onto $\varphi[R]$ and satisfies the additive properties for a homomorphism. For multiplication, $\mu[(a+H)(b+H)] = \mu(ab+H) = \varphi(ab) = \varphi(a)\varphi(b) = \mu(a+H)\mu(b+H)$. Therefore, μ is a one-to-one and onto homomorphism from R/H to $\varphi[R]$. That is, μ is an isomorphism, as claimed. □

Theorem 26.7 (continued 2)

Proof (continued). Next,

$$(a+H)((b+H)(c+H)) = (a+H)(b+c+H) = a(b+c)+H$$

$$= ab+ac+H = (ab+H)+(ac+H) = (a+H)(b+H)+(a+H)(c+H)$$

and left distribution holds, with right distribution follows similarly (R_3). Hence, R/H is a ring, as claimed.

Theorem 14.1 shows that the map μ defined in the theorem is well-defined, one-to-one, onto $\varphi[R]$ and satisfies the additive properties for a homomorphism. For multiplication, $\mu[(a+H)(b+H)] = \mu(ab+H) = \varphi(ab) = \varphi(a)\varphi(b) = \mu(a+H)\mu(b+H)$. Therefore, μ is a one-to-one and onto homomorphism from R/H to $\varphi[R]$. That is, μ is an isomorphism, as claimed. □

Theorem 26.9

Theorem 26.9 (Analogue of Theorem 14.4). Let H be a subring of the ring R. Multiplication of additive cosets of H is well defined by the equation $(a+H)(b+H) = ab + H$ if and only if $ah, hb \in H$ for all $a, b \in R$ and $h \in H$.

Proof. First, suppose that $ah, hb \in H$ for all $a, b \in R$ and all $h \in H$. Let $h_1, h_2 \in H$ so that $a + h_1$ and $b + h_2$ are also representatives of $a + H$ and $b + H$, respectively. Then $(a + h_1)(b + h_2) = ab + ah_2 + h_1 b + h_1 h_2$. Since, by hypothesis, $ah_2, h_1 b, h_1 h_2 \in H$, then $(a + h_1)(b + h_2) \in ab + H$. So the product is independent of the representatives and multiplication is well defined, as claimed.

Conversely, suppose that multiplication of additive cosets by representation is well defined. Let $a \in R$ and consider $(a + H)H$ using the representatives $a \in a + H$ and $0 \in H$. We have $(a + H)H = a0 + H = 0 + H = H$.

Theorem 26.9

Theorem 26.9 (Analogue of Theorem 14.4). Let H be a subring of the ring R. Multiplication of additive cosets of H is well defined by the equation $(a+H)(b+H) = ab + H$ if and only if $ah, hb \in H$ for all $a, b \in R$ and $h \in H$.

Proof. First, suppose that $ah, hb \in H$ for all $a, b \in R$ and all $h \in H$. Let $h_1, h_2 \in H$ so that $a + h_1$ and $b + h_2$ are also representatives of $a + H$ and $b + H$, respectively. Then $(a + h_1)(b + h_2) = ab + ah_2 + h_1 b + h_1 h_2$. Since, by hypothesis, $ah_2, h_1 b, h_1 h_2 \in H$, then $(a + h_1)(b + h_2) \in ab + H$. So the product is independent of the representatives and multiplication is well defined, as claimed.

Conversely, suppose that multiplication of additive cosets by representation is well defined. Let $a \in R$ and consider $(a + H)H$ using the representatives $a \in a + H$ and $0 \in H$. We have $(a + H)H = a0 + H = 0 + H = H$.

Theorem 26.9 (continued 1)

Theorem 26.9 (Analogue of Theorem 14.4). Let H be a subring of the ring R. Multiplication of additive cosets of H is well defined by the equation $(a+H)(b+H) = ab + H$ if and only if $ah, hb \in H$ for all $a, b \in R$ and $h \in H$.

Proof (continued). If we choose $a \in a + H$ and any $h \in H$ as representatives, we get $(a+H)H = a \cdot h + H$ and so $a + h + H = H$ and $ah \in H$ for any $h \in H$. Similarly, if we consider $H(b+H)$ using representatives $0 \in H$, $b \in b + H$ we get $H(b+H) = H$ and using representatives $b \in b + H$ and any $h \in H$ we get $H(b+H) = bh + H$. Hence $bh + H = H$ and $bh \in H$, as claimed. □

Theorem 26.9 (continued 1)

Theorem 26.9 (Analogue of Theorem 14.4). Let H be a subring of the ring R. Multiplication of additive cosets of H is well defined by the equation $(a+H)(b+H) = ab + H$ if and only if $ah, hb \in H$ for all $a, b \in R$ and $h \in H$.

Proof (continued). If we choose $a \in a + H$ and any $h \in H$ as representatives, we get $(a+H)H = a \cdot h + H$ and so $a + h + H = H$ and $ah \in H$ for any $h \in H$. Similarly, if we consider $H(b+H)$ using representatives $0 \in H$, $b \in b + H$ we get $H(b+H) = H$ and using representatives $b \in b + H$ and any $h \in H$ we get $H(b+H) = bh + H$. Hence $bh + H = H$ and $bh \in H$, as claimed. □

Theorem 26.14

Corollary 26.14. (Analogue of Corollary 14.5.)
Let N be an ideal of a ring R. Then the additive cosets of N form a ring R/N with the binary operations defined by
$(a + N) + (b + N) = (a + b) + N$ and $(a + N)(b + N) = ab + N$.

Proof. By Theorem 26.9, addition and multiplication are well-defined. We know that the additive cosets form an additive group, since ideal N is an additive subgroup of ring R, and so N is a normal subgroup since $\langle R, +\rangle$ is abelian (by Corollary 14.5).

Associativity and the distribution laws follow from the same properties in R (see the proof of Theorem 26.7 for $\mathcal{R}_2$ and $\mathcal{R}_3$). Hence R/N is a ring. □

Theorem 26.14

Corollary 26.14. (Analogue of Corollary 14.5.)
Let N be an ideal of a ring R. Then the additive cosets of N form a ring R/N with the binary operations defined by
$(a+N)+(b+N)=(a+b)+N$ and $(a+N)(b+N)=ab+N$.

Proof. By Theorem 26.9, addition and multiplication are well-defined. We know that the additive cosets form an additive group, since ideal N is an additive subgroup of ring R, and so N is a normal subgroup since $\langle R,+\rangle$ is abelian (by Corollary 14.5).

Associativity and the distribution laws follow from the same properties in R (see the proof of Theorem 26.7 for $\mathcal{R}_2$ and $\mathcal{R}_3$). Hence R/N is a ring. □

Theorem 26.16

Theorem 26.16 (Analogue of Theorem 14.9). Let N be an ideal of a ring R. Then $\gamma : R \to R/N$ given by $\gamma(x) = x + N$ is a ring homomorphism with kernel N.

Proof. The fact that $\gamma(x + y) = \gamma(x) + \gamma(y)$ for all $x, y \in R$ follows from Theorem 14.9. Now
$\gamma(x + y) = (xy) + N = (x + N)(y + N) = \gamma(x)\gamma(y)$ and so γ is a homomorphism. □

Theorem 26.17

Theorem 26.17. Fundamental Homomorphism Theorem (Analogue of Theorem 14.11)
Let $\varphi : R \to R'$ be a ring homomorphism with kernel N. Then $\varphi[R]$ is a ring and the map $\mu : R/N \to \varphi[R]$ given by $\mu(x + N) = \varphi(x)$ is an isomorphism. If $\gamma : R \to R/N$ is the homomorphism given by $\gamma(x) = x + N$ then for each $x \in R$, we have $\varphi(x) = (\mu\gamma)(x)$.

Proof. Theorem 26.16 shows that γ is a homomorphism and Theorem 26.7 shows that μ is an isomorphism. The result follows. □

Theorem 26.17

Theorem 26.17. Fundamental Homomorphism Theorem (Analogue of Theorem 14.11)
Let $\varphi : R \to R'$ be a ring homomorphism with kernel N. Then $\varphi[R]$ is a ring and the map $\mu : R/N \to \varphi[R]$ given by $\mu(x + N) = \varphi(x)$ is an isomorphism. If $\gamma : R \to R/N$ is the homomorphism given by $\gamma(x) = x + N$ then for each $x \in R$, we have $\varphi(x) = (\mu\gamma)(x)$.

Proof. Theorem 26.16 shows that γ is a homomorphism and Theorem 26.7 shows that μ is an isomorphism. The result follows. □