Introduction to Modern Algebra

Part III. Homomorphisms and Factor Groups

III.14. Factor Groups

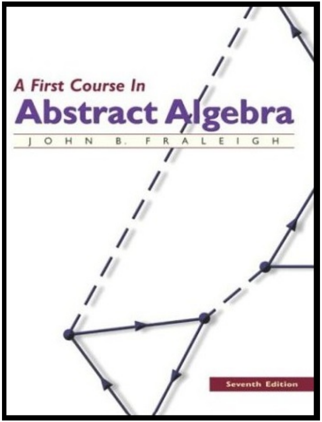

Table of contents

Theorem 14.1

Theorem 14.1. Let $\varphi : G \to G'$ be a group homomorphism with kernel $H = \text{Ker}(\varphi)$. Then the cosets of $H = \text{Ker}(\varphi)$. Then the cosests of $H = \text{Ker}(\varphi)$ from a *factor group*, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \varphi[G]$ defined by $\mu(aH) = \varphi(a)$ is an isomorphism. Both coset multiplication and μ are well defined (i.e., independent of the choices of a and b from the cosets).

Proof. Let $\varphi : G \to G'$ be a homomorphism with $H = \text{Ker}(\varphi)$. By Theorem 13.15, for any $a \in G$ we know that $aH = Ha$ so when we speak of "the cosets" of H, we can consider only the left cosets of H. Denote the set of all cosets of H as G/H. We now show that $\varphi : G/H \to \varphi[G]$ is a one-to-one mapping.

Theorem 14.1

Theorem 14.1. Let $\varphi : G \to G'$ be a group homomorphism with kernel $H = \text{Ker}(\varphi)$. Then the cosets of $H = \text{Ker}(\varphi)$. Then the cosests of $H = \text{Ker}(\varphi)$ from a *factor group*, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \varphi[G]$ defined by $\mu(aH) = \varphi(a)$ is an isomorphism. Both coset multiplication and μ are well defined (i.e., independent of the choices of a and b from the cosets).

Proof. Let $\varphi : G \to G'$ be a homomorphism with $H = \text{Ker}(\varphi)$. By Theorem 13.15, for any $a \in G$ we know that $aH = Ha$ so when we speak of "the cosets" of H, we can consider only the left cosets of H. Denote the set of all cosets of H as G/H. We now show that $\varphi : G/H \to \varphi[G]$ is a one-to-one mapping. Let $\varphi(a), \varphi(b) \in \varphi[G]$, $\varphi(a) \neq \varphi(b)$. Then by Theorem 13.15, $\varphi^{-1}[\{\varphi(a)\}] = \{x \in G \mid \varphi(x) = \varphi(a)\} = aH$. Since $\varphi(a) \neq \varphi(b)$ then aH and bH are disjoint. That is, $aH \neq bH$. So $\varphi : G/H \to \varphi[G]$ is one-to-one, as claimed.

Theorem 14.1

Theorem 14.1. Let $\varphi : G \to G'$ be a group homomorphism with kernel $H = \text{Ker}(\varphi)$. Then the cosets of $H = \text{Ker}(\varphi)$. Then the cosests of $H = \text{Ker}(\varphi)$ from a *factor group*, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \varphi[G]$ defined by $\mu(aH) = \varphi(a)$ is an isomorphism. Both coset multiplication and μ are well defined (i.e., independent of the choices of a and b from the cosets).

Proof. Let $\varphi : G \to G'$ be a homomorphism with $H = \text{Ker}(\varphi)$. By Theorem 13.15, for any $a \in G$ we know that $aH = Ha$ so when we speak of "the cosets" of H, we can consider only the left cosets of H. Denote the set of all cosets of H as G/H. We now show that $\varphi : G/H \to \varphi[G]$ is a one-to-one mapping. Let $\varphi(a), \varphi(b) \in \varphi[G]$, $\varphi(a) \neq \varphi(b)$. Then by Theorem 13.15, $\varphi^{-1}[\{\varphi(a)\}] = \{x \in G \mid \varphi(x) = \varphi(a)\} = aH$. Since $\varphi(a) \neq \varphi(b)$ then aH and bH are disjoint. That is, $aH \neq bH$. So $\varphi : G/H \to \varphi[G]$ is one-to-one, as claimed.

Theorem 14.1 (continued 1)

Proof (continued). We claim $\varphi : G/H \to \varphi[G]$ is onto. Let $\varphi(g) \circ \varphi[G]$ for some $g \in G$. Then $\varphi(gH) = g$ for coset $ghH \in G/H$ and φ is onto, as claimed.

Next, we define a binary operation on G/H as: For $aH, bH \in G/H$, define $(aH) \cdot (bH) = (aH)(bH) = (ab)H$. First, we show that $\cdot$ is well-defined (that is, it is independent of the choice of $a, b \in G$). Let $a_1 \in aH$ and $b_1 \in bH$. Then $a_1 = ah_1$ and $b_1 = bh_2$ for some $h_1, h_2 \in H$. There exists $h_3 \in H$ such that $h_1 b = bh_3$ since $aH = Ha$ by Theorem 13.15 (this is where the fact that the cosets coincide is used—in insuring that the binary operation on G/H is well defined).

Theorem 14.1 (continued 1)

Proof (continued). We claim $\varphi : G/H \to \varphi[G]$ is onto. Let $\varphi(g) \circ \varphi[G]$ for some $g \in G$. Then $\varphi(gH) = g$ for coset $ghH \in G/H$ and φ is onto, as claimed.

Next, we define a binary operation on G/H as: For $aH, bH \in G/H$, define $(aH) \cdot (bH) = (aH)(bH) = (ab)H$. First, we show that $\cdot$ is well-defined (that is, it is independent of the choice of $a, b \in G$). Let $a_1 \in aH$ and $b_1 \in bH$. Then $a_1 = ah_1$ and $b_1 = bh_2$ for some $h_1, h_2 \in H$. There exists $h_3 \in H$ such that $h_1 b = bh_3$ since $aH = Ha$ by Theorem 13.15 (this is where the fact that the cosets coincide is used—in insuring that the binary operation on G/H is well defined). Hence

$$a_1 b_1 = (ah_1)(bh_2) = a(h_1 b)h_2 = a(bh_3)h_2 = (ab)(h_3 h_2) \in (ab)H.$$

So $(a_1 b_1)H \subset (ab)H$ and similarly $(ab)H \subset (a_1 b_1)H$. That is, $(ab)H = (a_1 b_1)H$ and $\cdot$ is well defined, as claimed.

Theorem 14.1 (continued 1)

Proof (continued). We claim $\varphi : G/H \to \varphi[G]$ is onto. Let $\varphi(g) \circ \varphi[G]$ for some $g \in G$. Then $\varphi(gH) = g$ for coset $ghH \in G/H$ and φ is onto, as claimed.

Next, we define a binary operation on G/H as: For $aH, bH \in G/H$, define $(aH) \cdot (bH) = (aH)(bH) = (ab)H$. First, we show that $\cdot$ is well-defined (that is, it is independent of the choice of $a, b \in G$). Let $a_1 \in aH$ and $b_1 \in bH$. Then $a_1 = ah_1$ and $b_1 = bh_2$ for some $h_1, h_2 \in H$. There exists $h_3 \in H$ such that $h_1 b = bh_3$ since $aH = Ha$ by Theorem 13.15 (this is where the fact that the cosets coincide is used—in insuring that the binary operation on G/H is well defined). Hence

$$a_1 b_1 = (ah_1)(bh_2) = a(h_1 b)h_2 = a(bh_3)h_2 = (ab)(h_3 h_2) \in (ab)H.$$

So $(a_1 b_1)H \subset (ab)H$ and similarly $(ab)H \subset (a_1 b_1)H$. That is, $(ab)H = (a_1 b_1)H$ and $\cdot$ is well defined, as claimed.

Theorem 14.1 (continued 2)

Proof (continued). We claim that since G is a group, the $\langle G/H, \cdot \rangle$ is a group. First, $((aH)\cdot(bH))\cdot(cH) = ((ab)H)\cdot(cH) = (abc)H = (aH)\cdot((bc)H) = (aH)(bH\cdot cH)$ and so $\cdot$ is associative and $\mathcal{G}_1$ holds. Second, for all $a \in G$, $(eH)\cdot(aH) = (ea)H = aH$, so $eH = H$ is the identity of G/H and $\mathcal{G}_2$ holds. Third, for all $a \in G$ we have $(aH)\cdot(a^{-1}H) = (aa^{-1})H = eH = H$ and $\mathcal{G}_3$ holds. So $\langle G/H, \cdot \rangle$ is a group, as claimed.

Finally, we show that $\mu : G/H \to \varphi[G]$ defined as $\mu(aH) = \varphi(a)$ is an isomorphism. First, we must show that μ is well-defined (that is, independent of the choice of $a \in aH$). Let $a_1 \in aH$. Then by Theorem 13.15, $aH = \varphi^{-1}[\{\varphi(a)\}] = \{x \in G \mid \varphi(x) = \varphi(a)\} = \{x \in G \mid \varphi(x) = \varphi(a_1)\} = a_1H$.

Theorem 14.1 (continued 2)

Proof (continued). We claim that since G is a group, the $\langle G/H, \cdot\rangle$ is a group. First, $((aH)\cdot(bH))\cdot(cH) = ((ab)H)\cdot(cH) = (abc)H = (aH)\cdot((bc)H) = (aH)(bH\cdot cH)$ and so $\cdot$ is associative and $\mathcal{G}_1$ holds. Second, for all $a \in G$, $(eH)\cdot(aH) = (ea)H = aH$, so $eH = H$ is the identity of G/H and $\mathcal{G}_2$ holds. Third, for all $a \in G$ we have $(aH)\cdot(a^{-1}H) = (aa^{-1})H = eH = H$ and $\mathcal{G}_3$ holds. So $\langle G/H, \cdot\rangle$ is a group, as claimed.

Finally, we show that $\mu : G/H \to \varphi[G]$ defined as $\mu(aH) = \varphi(a)$ is an isomorphism. First, we must show that μ is well-defined (that is, independent of the choice of $a \in aH$). Let $a_1 \in aH$. Then by Theorem 13.15, $aH = \varphi^{-1}[\{\varphi(a)\}] = \{x \in G \mid \varphi(x) = \varphi(a)\} = \{x \in G \mid \varphi(x) = \varphi(a_1)\} = a_1H$. Therefore $\mu(aH) = \varphi(a) = \varphi(a_1) = \mu(a_1H)$ and μ is well defined. Notice next that $\mu(aH) = \varphi[aH]$ as defined above. Since $\varphi : G/H \to \varphi[G]$ is one-to-one and onto as shown above, then $\mu : G/H \to \varphi[G]$ is one-to-one and onto. That is, μ is an isomorphism and G/H is isomorphic to $\varphi[G]$, as claimed. □

Theorem 14.1 (continued 2)

Proof (continued). We claim that since G is a group, the $\langle G/H, \cdot \rangle$ is a group. First, $((aH) \cdot (bH)) \cdot (cH) = ((ab)H) \cdot (cH) = (abc)H = (aH) \cdot ((bc)H) = (aH)(bH \cdot cH)$ and so $\cdot$ is associative and G_1 holds. Second, for all $a \in G$, $(eH) \cdot (aH) = (ea)H = aH$, so $eH = H$ is the identity of G/H and G_2 holds. Third, for all $a \in G$ we have $(aH) \cdot (a^{-1}H) = (aa^{-1})H = eH = H$ and G_3 holds. So $\langle G/H, \cdot \rangle$ is a group, as claimed.

Finally, we show that $\mu : G/H \to \varphi[G]$ defined as $\mu(aH) = \varphi(a)$ is an isomorphism. First, we must show that μ is well-defined (that is, independent of the choice of $a \in aH$). Let $a_1 \in aH$. Then by Theorem 13.15, $aH = \varphi^{-1}[\{\varphi(a)\}] = \{x \in G \mid \varphi(x) = \varphi(a)\} = \{x \in G \mid \varphi(x) = \varphi(a_1)\} = a_1 H$. Therefore $\mu(aH) = \varphi(a) = \varphi(a_1) = \mu(a_1 H)$ and μ is well defined. Notice next that $\mu(aH) = \varphi[aH]$ as defined above. Since $\varphi : G/H \to \varphi[G]$ is one-to-one and onto as shown above, then $\mu : G/H \to \varphi[G]$ is one-to-one and onto. That is, μ is an isomorphism and G/H is isomorphic to $\varphi[G]$, as claimed. □

Theorem 14.4

Theorem 14.4. Let H be a subgroup of a group G. Then left coset multiplication is well-defined by the equation $(aH) \cdot (bH) = (ab)H$ if and only if H is a normal subgroup of G.

Proof. First, assume $(aH) \cdot (bH) = (ab)H$ is a well-defined binary operation on left cosets. Let $a \in G$. We now show $aH = Ha$ (and so H is a normal subgroup of G). Let $x \in aH$. We have $a^{-1} \in a^{-1}H$ and so $(xH) \cdot (a^{-1}H) = (xa^{-1}H)$. Also, $a \in aH$ and so $(aH) \cdot (a^1 H) = (aa^1) = eH = H$.

Theorem 14.4

Theorem 14.4. Let H be a subgroup of a group G. Then left coset multiplication is well-defined by the equation $(aH) \cdot (bH) = (ab)H$ if and only if H is a normal subgroup of G.

Proof. First, assume $(aH) \cdot (bH) = (ab)H$ is a well-defined binary operation on left cosets. Let $a \in G$. We now show $aH = Ha$ (and so H is a normal subgroup of G). Let $x \in aH$. We have $a^{-1} \in a^{-1}H$ and so $(xH) \cdot (a^{-1}H) = (xa^{-1}H)$. Also, $a \in aH$ and so $(aH) \cdot (a^1 H) = (aa^1) = eH = H$. If $\cdot$ is well defined then we must have $(xH) \cdot (a^{-1}H) = (aH) \cdot (a^{-1}H)$ (since both x and a can be used as representatives of coset aH), that $(xa^{-1})H = eH = H$ and so $xa^{-1} = h \in H$. Then $x = ha$ and $x \in Ha$. Therefore $aH \subset Ha$.

Theorem 14.4

Theorem 14.4. Let H be a subgroup of a group G. Then left coset multiplication is well-defined by the equation $(aH) \cdot (bH) = (ab)H$ if and only if H is a normal subgroup of G.

Proof. First, assume $(aH) \cdot (bH) = (ab)H$ is a well-defined binary operation on left cosets. Let $a \in G$. We now show $aH = Ha$ (and so H is a normal subgroup of G). Let $x \in aH$. We have $a^{-1} \in a^{-1}H$ and so $(xH) \cdot (a^{-1}H) = (xa^{-1}H)$. Also, $a \in aH$ and so $(aH) \cdot (a^1 H) = (aa^1) = eH = H$. If $\cdot$ is well defined then we must have $(xH) \cdot (a^{-1}H) = (aH) \cdot (a^{-1}H)$ (since both x and a can be used as representatives of coset aH), that $(xa^{-1})H = eH = H$ and so $xa^{-1} = h \in H$. Then $x = ha$ and $x \in Ha$. Therefore $aH \subset Ha$. Next, let $y \in Ha$ (this part is Exercise 14.25). Then $y = ha$ for some $h \in H$. In this left coset product $(a^{-1}H) \cdot (aH)$, choose $a^{-1}h \in a^{-1}H$ and $a \in aH$ for the representatives to get $(a^{-1}hH) \cdot (aH) = (a^{-1}ha)H$ and since $(a^{-1}H) \cdot (aH) = (a^{-1}a)H = eH = H$ ($\cdot$ is well defined), it must be that $a^{-1}ha = h'$ for some $h' \in H$.

Theorem 14.4

Theorem 14.4. Let H be a subgroup of a group G. Then left coset multiplication is well-defined by the equation $(aH) \cdot (bH) = (ab)H$ if and only if H is a normal subgroup of G.

Proof. First, assume $(aH) \cdot (bH) = (ab)H$ is a well-defined binary operation on left cosets. Let $a \in G$. We now show $aH = Ha$ (and so H is a normal subgroup of G). Let $x \in aH$. We have $a^{-1} \in a^{-1}H$ and so $(xH) \cdot (a^{-1}H) = (xa^{-1}H)$. Also, $a \in aH$ and so $(aH) \cdot (a^{1}H) = (aa^{1}) = eH = H$. If $\cdot$ is well defined then we must have $(xH) \cdot (a^{-1}H) = (aH) \cdot (a^{-1}H)$ (since both x and a can be used as representatives of coset aH), that $(xa^{-1})H = eH = H$ and so $xa^{-1} = h \in H$. Then $x = ha$ and $x \in Ha$. Therefore $aH \subset Ha$. Next, let $y \in Ha$ (this part is Exercise 14.25). Then $y = ha$ for some $h \in H$. In this left coset product $(a^{-1}H) \cdot (aH)$, choose $a^{-1}h \in a^{-1}H$ and $a \in aH$ for the representatives to get $(a^{-1}hH) \cdot (aH) = (a^{-1}ha)H$ and since $(a^{-1}H) \cdot (aH) = (a^{-1}a)H = eH = H$ ($\cdot$ is well defined), it must be that $a^{-1}ha = h'$ for some $h' \in H$.

Theorem 14.4 (continued)

Proof (continued). Then, $ha = ah'$ for some $h' \in H$. That is, $y = ha \in aH$. Therefore $Ha \subset aH$. Combining this with the result above, gives $aH = Ha$ and we have that the cosets of H coincide. Therefore, H is a normal subgroup of G.

Second, suppose H is a normal subgroup of G and so left and right cosets coincide. Consider a coset product $((ah_1)H) \cdot ((bh_2)H) = (ah_1bh_2)H$. So to show that $\cdot$ is well defined, we need to show that $(ah_1bh_2)H = (ab)H$.

Theorem 14.4 (continued)

Proof (continued). Then, $ha = ah'$ for some $h' \in H$. That is, $y = ha \in aH$. Therefore $Ha \subset aH$. Combining this with the result above, gives $aH = Ha$ and we have that the cosets of H coincide. Therefore, H is a normal subgroup of G.

Second, suppose H is a normal subgroup of G and so left and right cosets coincide. Consider a coset product $((ah_1)H) \cdot ((bh_2)H) = (ah_1bh_2)H$. So to show that $\cdot$ is well defined, we need to show that $(ah_1bh_2)H = (ab)H$. Now $h_1b \in Hb = bH$ (by hypothesis) and so $h_1b = bh_3$ for some $h_3 \in H$. Therefore $(ah_1)(bh_2)H \cap (ab)H \neq \emptyset$. Since the left cosets of H partition group G (Section II.10) then different cosets disjoint. So $(ah_1bh_2)H = (ab)H$ and $(aH) \cdot (bH) = ((ah_1)H) \cdot ((bh_2)H)$. That is, $\cdot$ is well defined. □

Theorem 14.4 (continued)

Proof (continued). Then, $ha = ah'$ for some $h' \in H$. That is, $y = ha \in aH$. Therefore $Ha \subset aH$. Combining this with the result above, gives $aH = Ha$ and we have that the cosets of H coincide. Therefore, H is a normal subgroup of G.

Second, suppose H is a normal subgroup of G and so left and right cosets coincide. Consider a coset product $((ah_1)H) \cdot ((bh_2)H) = (ah_1bh_2)H$. So to show that $\cdot$ is well defined, we need to show that $(ah_1bh_2)H = (ab)H$. Now $h_1b \in Hb = bH$ (by hypothesis) and so $h_1b = bh_3$ for some $h_3 \in H$. Therefore $(ah_1)(bh_2)H \cap (ab)H \neq \emptyset$. Since the left cosets of H partition group G (Section II.10) then different cosets disjoint. So $(ah_1bh_2)H = (ab)H$ and $(aH) \cdot (bH) = ((ah_1)H) \cdot ((bh_2)H)$. That is, $\cdot$ is well defined. □

Corollary 14.5

Corollary 14.5. Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH) \cdot (bH) = (ab)H$.

Proof. First, $(aH) \cdot [(bH) \cdot (cH)] = (aH) \cdot ((bc)H) = (abc)H$ and $[(aH) \cdot (bH)] \cdot (cH) = ((ab)H) \cdot (cH) = (abc)H$, and so $\cdot$ is associative and G_1 holds.

Corollary 14.5

Corollary 14.5. Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH) \cdot (bH) = (ab)H$.

Proof. First, $(aH) \cdot [(bH) \cdot (cH)] = (aH) \cdot ((bc)H) = (abc)H$ and $[(aH) \cdot (bH)] \cdot (cH) = ((ab)H) \cdot (cH) = (abc)H$, and so $\cdot$ is associative and G_1 holds.

Second, for all $ah \in G/H$, $(aH) \cdot (eH) = (ae)H = aH$ and G_2 holds (it is sufficient to consider one sided identities and inverses by page 43 and Exercise 4.38).

Corollary 14.5

Corollary 14.5. Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH) \cdot (bH) = (ab)H$.

Proof. First, $(aH) \cdot [(bH) \cdot (cH)] = (aH) \cdot ((bc)H) = (abc)H$ and $[(aH) \cdot (bH)] \cdot (cH) = ((ab)H) \cdot (cH) = (abc)H$, and so $\cdot$ is associative and G_1 holds.

Second, for all $ah \in G/H$, $(aH) \cdot (eH) = (ae)H = aH$ and G_2 holds (it is sufficient to consider one sided identities and inverses by page 43 and Exercise 4.38).

Third, for all $aH \in G/H$, $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$ and $(aH)^{-1} = (a^{-1})H$; so G_3 holds. □

Corollary 14.5

Corollary 14.5. Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH) \cdot (bH) = (ab)H$.

Proof. First, $(aH) \cdot [(bH) \cdot (cH)] = (aH) \cdot ((bc)H) = (abc)H$ and $[(aH) \cdot (bH)] \cdot (cH) = ((ab)H) \cdot (cH) = (abc)H$, and so $\cdot$ is associative and G_1 holds.

Second, for all $ah \in G/H$, $(aH) \cdot (eH) = (ae)H = aH$ and G_2 holds (it is sufficient to consider one sided identities and inverses by page 43 and Exercise 4.38).

Third, for all $aH \in G/H$, $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$ and $(aH)^{-1} = (a^{-1})H$; so G_3 holds. □

Theorem 14.9

Theorem 14.9. Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

Proof. Let $x, y \in G$. Then

$$\gamma(xy) = (xy)H = (xH) \cdot (yH) = \gamma(x)\gamma(y),$$

and so γ is a homomorphism. Now $xH = H$ if and only if $x \in H$ (recall that distinct cosets are disjoint) and so $\gamma(x) = xH = H = \gamma(e)$ if and only if $x \in H$—that is, the kernel of γ is H. □

Theorem 14.9

Theorem 14.9. Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

Proof. Let $x, y \in G$. Then

$$\gamma(xy) = (xy)H = (xH) \cdot (yH) = \gamma(x)\gamma(y),$$

and so γ is a homomorphism. Now $xH = H$ if and only if $x \in H$ (recall that distinct cosets are disjoint) and so $\gamma(x) = xH = H = \gamma(e)$ if and only if $x \in H$—that is, the kernel of γ is H. □

Theorem 14.11. The Fundamental Homomorphism Theorem

Theorem 14.11. The Fundamental Homomorphism Theorem.
Let $\varphi : G \to G'$ be a group homomorphism with kernel H, and let $\gamma : G \to G/H$ be the homomorphism given by $\gamma(g) = gH$ of Theorem 14.9. Then:

1. $\varphi[G]$ is a group,
2. $\mu : G/H \to \varphi[G]$ given by $\mu(gH) = \varphi(g)$ is an isomorphism, and
3. $\varphi(g) = \mu(\gamma(g)) = \mu \circ \gamma(g)$ for each $g \in G$.

μ is called the *canonical* (or *natural*) *isomorphism* between G/H and $\varphi[G]$. γ is similarly the *canonical* (or *natural*) *homomorphism* between G and G/H.

Proof. $\varphi[G]$ is a group by Theorem 13.12 Part (3). μ is an isomorphism by Theorem 14.1. For $g \in G$, $\mu(\gamma(g)) = \mu(gH) = \varphi(g)$ by the definitions of μ and γ. □

Theorem 14.11. The Fundamental Homomorphism Theorem

Theorem 14.11. The Fundamental Homomorphism Theorem.
Let $\varphi : G \to G'$ be a group homomorphism with kernel H, and let $\gamma : G \to G/H$ be the homomorphism given by $\gamma(g) = gH$ of Theorem 14.9. Then:

1. $\varphi[G]$ is a group,
2. $\mu : G/H \to \varphi[G]$ given by $\mu(gH) = \varphi(g)$ is an isomorphism, and
3. $\varphi(g) = \mu(\gamma(g)) = \mu \circ \gamma(g)$ for each $g \in G$.

μ is called the *canonical* (or *natural*) *isomorphism* between G/H and $\varphi[G]$. γ is similarly the *canonical* (or *natural*) *homomorphism* between G and G/H.

Proof. $\varphi[G]$ is a group by Theorem 13.12 Part (3). μ is an isomorphism by Theorem 14.1. For $g \in G$, $\mu(\gamma(g)) = \mu(gH) = \varphi(g)$ by the definitions of μ and γ. □

Exercise 14.6

Exercise 14.6. Find the order of $\mathbb{Z}_{12} \times \mathbb{Z}_{18} / \langle (4,3) \rangle$.

Solution. Notice that $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ is abelian, and so $H = \langle (4,3) \rangle$ is a normal subgroup. Now, $\mathbb{Z}_{12} \times \mathbb{Z}_{18} / \langle (4,3) \rangle$ is the group of cosets of $H = \langle (4,3) \rangle$. Since $|H| = 6$ and all cosets of H are the same size (Section II.10), then the number of cosets is $|\mathbb{Z}_{12} \times \mathbb{Z}_{18}|/|H| = 12 \times 18/6 = 36$. In Section II.10, the number of cosets is the index $(G : H)$ and equals $|G|/|H|$ when $|G|$ is finite, so this technique works for general finite factor groups. □

Exercise 14.6

Exercise 14.6. Find the order of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}/\langle(4,3)\rangle$.

Solution. Notice that $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ is abelian, and so $H = \langle(4,3)\rangle$ is a normal subgroup. Now, $\mathbb{Z}_{12} \times \mathbb{Z}_{18}/\langle(4,3)\rangle$ is the group of cosets of $H = \langle(4,3)\rangle$. Since $|H| = 6$ and all cosets of H are the same size (Section II.10), then the number of cosets is $|\mathbb{Z}_{12} \times \mathbb{Z}_{18}|/|H| = 12 \times 18/6 = 36$. In Section II.10, the number of cosets is the index $(G : H)$ and equals $|G|/|H|$ when $|G|$ is finite, so this technique works for general finite factor groups. □

Theorem 14.13

Theorem.14.13. Let G be group and H a subgroup of G. The following are equivalent

1. $gH = Hg$ for all $g \in G$ (that is, H is normal subgroup).
2. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$
3. $gHg^{-1} = H$ for all $g \in G$.

Proof. Suppose (2) holds and H is a subgroup of G such that $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. Then $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \subseteq H$ for all $g \in G$. Let $h \in H$. Then by the hypothesis of (2), $g^{-1}hg \in H$, or $g^{-1}hg = h_1$ for some $h_1 \in H$. Then $h = gh_1g^{-1}$ and $h \in gHg^{-1}$. So $H \subseteq gHg^{-1}$. Therefore $H = gHg^{-1}$ and (2) implies (3).

Theorem 14.13

Theorem.14.13. Let G be group and H a subgroup of G. The following are equivalent

1. $gH = Hg$ for all $g \in G$ (that is, H is normal subgroup).
2. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$
3. $gHg^{-1} = H$ for all $g \in G$.

Proof. Suppose (2) holds and H is a subgroup of G such that $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. Then $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \subseteq H$ for all $g \in G$. Let $h \in H$. Then by the hypothesis of (2), $g^{-1}hg \in H$, or $g^{-1}hg = h_1$ for some $h_1 \in H$. Then $h = gh_1g^{-1}$ and $h \in gHg^{-1}$. So $H \subseteq gHg^{-1}$. Therefore $H = gHg^{-1}$ and (2) implies (3).

Theorem 14.13 (continued).

Proof (continued). Suppose (1) holds and H is a normal subgroup of G : $gH = Hg$ for all $g \in G$. Let $g \in G$ and $h \in G$. Then for some $h_1 \in H$ we have $gh = h_1 g$ or $ghg^{-1} = h_1$ and so $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. That is, (1) implies (2).

Suppose (3) holds and $gHg^{-1} = H$, we similarly have $g^{-1}H \subseteq Hg^{-1}$ or equivalently $Hg \subseteq gH$. So $gH = Hg$ and (3) implies (1). Hence we have the implications (1) implies (2) implies (3) implies (1), and so all statements (1), (2), (3) are equivalent, as claimed. □

Theorem 14.13 (continued).

Proof (continued). Suppose (1) holds and H is a normal subgroup of G : $gH = Hg$ for all $g \in G$. Let $g \in G$ and $h \in G$. Then for some $h_1 \in H$ we have $gh = h_1 g$ or $ghg^{-1} = h_1$ and so $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. That is, (1) implies (2).

Suppose (3) holds and $gHg^{-1} = H$, we similarly have $g^{-1}H \subseteq Hg^{-1}$ or equivalently $Hg \subseteq gH$. So $gH = Hg$ and (3) implies (1). Hence we have the implications (1) implies (2) implies (3) implies (1), and so all statements (1), (2), (3) are equivalent, as claimed. □

Exercise 13.29

Exercise 13.29. Let G be a group and let $g \in G$. Let $i_g : G \to G$ be defined by $i_g(x) = gxg^{-1}$ for $x \in G$. Then i_g is an automorphism of G.

Proof. First, we show i_g is a homomorphism for all $g \in G$. Let $x, y \in G$. Then $i_g(xy) = g(xy)g^{-1} = g(xey)g^{-1} = g(x(g^{-1}g))yg^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$.

Exercise 13.29

Exercise 13.29. Let G be a group and let $g \in G$. Let $i_g : G \to G$ be defined by $i_g(x) = gxg^{-1}$ for $x \in G$. Then i_g is an automorphism of G.

Proof. First, we show i_g is a homomorphism for all $g \in G$. Let $x, y \in G$. Then $i_g(xy) = g(xy)g^{-1} = g(xey)g^{-1} = g(x(g^{-1}g))yg^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$.

Next, suppose $i_g(x) = i_g(y)$. Then

$$gxg^{-1} = gyg^{-1} \text{ or } xg^{-1} = yg^{-1},$$

by left cancellation and $x = y$ by right cancellation. So i_g is one-to-one.

Exercise 13.29

Exercise 13.29. Let G be a group and let $g \in G$. Let $i_g : G \to G$ be defined by $i_g(x) = gxg^{-1}$ for $x \in G$. Then i_g is an automorphism of G.

Proof. First, we show i_g is a homomorphism for all $g \in G$. Let $x, y \in G$. Then $i_g(xy) = g(xy)g^{-1} = g(xey)g^{-1} = g(x(g^{-1}g))yg^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$.

Next, suppose $i_g(x) = i_g(y)$. Then

$$gxg^{-1} = gyg^{-1} \text{ or } xg^{-1} = yg^{-1},$$

by left cancellation and $x = y$ by right cancellation. So i_g is one-to-one.

Finally let $y \in G$. Then $g^{-1}yg \in G$ and $i_g(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y$ and so i_g is onto. Therefore i_g is an isomorphism from G to G - that is is i_g is an automorphism of G. □

Exercise 13.29

Exercise 13.29. Let G be a group and let $g \in G$. Let $i_g : G \rightarrow G$ be defined by $i_g(x) = gxg^{-1}$ for $x \in G$. Then i_g is an automorphism of G.

Proof. First, we show i_g is a homomorphism for all $g \in G$. Let $x, y \in G$. Then $i_g(xy) = g(xy)g^{-1} = g(xey)g^{-1} = g(x(g^{-1}g))yg^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$.

Next, suppose $i_g(x) = i_g(y)$. Then

$$gxg^{-1} = gyg^{-1} \text{ or } xg^{-1} = yg^{-1},$$

by left cancellation and $x = y$ by right cancellation. So i_g is one-to-one.

Finally let $y \in G$. Then $g^{-1}yg \in G$ and $i_g(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y$ and so i_g is onto. Therefore i_g is an isomorphism from G to G - that is is i_g is an automorphism of G. □