Introduction to Modern Algebra

Part II. Permutations, Cosets, and Direct Products

II.8. Groups of Permutations

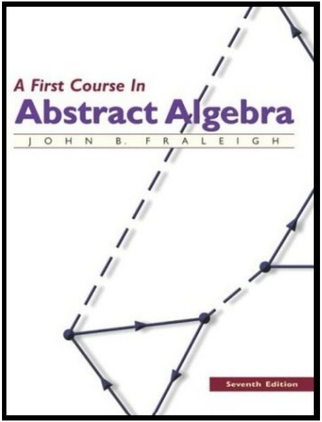

Table of contents

Lemma

Lemma. If σ and τ are permutations on set A, then the composite function $\sigma \circ \tau$ (defined as $A \xrightarrow{\tau} A \xrightarrow{\sigma} A$ is a permutation on A. Normally we drop the composition symbol $\circ$ and write $\sigma \circ \tau = \sigma\tau$. Notice that we must read this from right to left since $\sigma\tau$ is permutation τ first, followed by permutation σ.

Proof. We must only show that $\sigma\tau$ is one-to-one and onto. For one-to-one (see page 4 for the definition), suppose $(\sigma\tau)(a_1) = (\sigma\tau)(a_2)$; that is, $\sigma(\tau(a_1)) = \sigma(\tau(a_2))$. Since σ is one-to-one, then the two "inputs" of τ must be the same and so $a_1 = a_2$. Therefore $\sigma\tau$ is one to one.

Lemma

Lemma. If σ and τ are permutations on set A, then the composite function $\sigma \circ \tau$ (defined as $A \xrightarrow{\tau} A \xrightarrow{\sigma} A$ is a permutation on A. Normally we drop the composition symbol $\circ$ and write $\sigma \circ \tau = \sigma\tau$. Notice that we must read this from right to left since $\sigma\tau$ is permutation τ first, followed by permutation σ.

Proof. We must only show that $\sigma\tau$ is one-to-one and onto. For one-to-one (see page 4 for the definition), suppose $(\sigma\tau)(a_1) = (\sigma\tau)(a_2)$; that is, $\sigma(\tau(a_1)) = \sigma(\tau(a_2))$. Since σ is one-to-one, then the two "inputs" of τ must be the same and so $a_1 = a_2$. Therefore $\sigma\tau$ is one to one.

For onto, let $a \in A$. Since σ is onto A, then there is some $a' \in A$ such that $\sigma(a') = a$. Since τ is onto A, there is some $a'' \in A$ such that $\tau(a'') = a'$. Then $a = \sigma(a') = \sigma(\tau(a'')) = (\sigma\tau)(a'')$ and so $\sigma\tau$ is onto A. □

Lemma

Lemma. If σ and τ are permutations on set A, then the composite function $\sigma \circ \tau$ (defined as $A \xrightarrow{\tau} A \xrightarrow{\sigma} A$ is a permutation on A. Normally we drop the composition symbol $\circ$ and write $\sigma \circ \tau = \sigma\tau$. Notice that we must read this from right to left since $\sigma\tau$ is permutation τ first, followed by permutation σ.

Proof. We must only show that $\sigma\tau$ is one-to-one and onto. For one-to-one (see page 4 for the definition), suppose $(\sigma\tau)(a_1) = (\sigma\tau)(a_2)$; that is, $\sigma(\tau(a_1)) = \sigma(\tau(a_2))$. Since σ is one-to-one, then the two "inputs" of τ must be the same and so $a_1 = a_2$. Therefore $\sigma\tau$ is one to one.

For onto, let $a \in A$. Since σ is onto A, then there is some $a' \in A$ such that $\sigma(a') = a$. Since τ is onto A, there is some $a'' \in A$ such that $\tau(a'') = a'$. Then $a = \sigma(a') = \sigma(\tau(a'')) = (\sigma\tau)(a'')$ and so $\sigma\tau$ is onto A. □

Theorem 8.5.

Theorem 8.5. Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

Proof. By Lemma, we know that the product of two permutations of set A are again a permutation of set A. So S_A is closed under multiplication.

Theorem 8.5.

Theorem 8.5. Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

Proof. By Lemma, we know that the product of two permutations of set A are again a permutation of set A. So S_A is closed under multiplication. We now show that S_A is a group. Since permutations multiplication is defined as function composition and function composition is associative by Theorem 2.13, then S_A satisfies property G_1 of the definition of group.

The identity permutation is ι defined as $\iota(a) = a$ for all $a \in A$, since $\sigma_i = \iota\sigma = \sigma$ for all $\sigma \in S_A$. So G_2 is satisfied.

Theorem 8.5.

Theorem 8.5. Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

Proof. By Lemma, we know that the product of two permutations of set A are again a permutation of set A. So S_A is closed under multiplication. We now show that S_A is a group. Since permutations multiplication is defined as function composition and function composition is associative by Theorem 2.13, then S_A satisfies property G_1 of the definition of group.

The identity permutation is ι defined as $\iota(a) = a$ for all $a \in A$, since $\sigma_i = \iota\sigma = \sigma$ for all $\sigma \in S_A$. So G_2 is satisfied.

For $\sigma \in S_A$, define σ' on A as $\sigma'(a') = a$ if and only if $\sigma'(a) = a'$ for each $a \in A$. Since σ is one-to-one and onto A, σ' is well defined, one-to-one and onto.

Theorem 8.5.

Theorem 8.5. Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

Proof. By Lemma, we know that the product of two permutations of set A are again a permutation of set A. So S_A is closed under multiplication. We now show that S_A is a group. Since permutations multiplication is defined as function composition and function composition is associative by Theorem 2.13, then S_A satisfies property G_1 of the definition of group.

The identity permutation is ι defined as $\iota(a) = a$ for all $a \in A$, since $\sigma_i = \iota\sigma = \sigma$ for all $\sigma \in S_A$. So G_2 is satisfied.

For $\sigma \in S_A$, define σ' on A as $\sigma'(a') = a$ if and only if $\sigma'(a) = a'$ for each $a \in A$. Since σ is one-to-one and onto A, σ' is well defined, one-to-one and onto.

Theorem 8.5 (continued).

Theorem 8.5 Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

Proof (continued). For each $a \in A$ we have

$$\iota(a) = a = \sigma'(a') = \sigma'(\sigma(a)) = (\sigma'\sigma)(a)$$

and

$$\iota(a') = a' = \sigma(a) = \sigma(\sigma'(a')) = (\sigma\sigma')(a')$$

and so $\sigma'\sigma = \sigma\sigma' = \iota$. That is, σ' is the inverse of σ (we denote $\sigma' = \sigma^{-1}$), and G_3 is satisfied. □

Lemma 8.15.

Lemma 8.15. Let G and G' be groups and let $\varphi : G \to G'$ be a one-to-one function such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$. then $\varphi[G]$ is a subgroup of G' and φ is an isomorphism of G with $\varphi[G]$.

Proof. We use Theorem 5.14. Let $x', y' \in \varphi[G]$. Then for for some $x, y \in G$ we have $x' = \varphi(x)$ and $y' = \varphi(y)$. So $x, y \in G$ and so $x'y' = \varphi(x)\varphi(y) = \varphi(xy)$ (by hypothesis), and so $x'y' \in \varphi[G]$. That is, $\varphi[G]$ is closed under the binary operation of G'.

Lemma 8.15.

Lemma 8.15. Let G and G' be groups and let $\varphi : G \to G'$ be a one-to-one function such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$. then $\varphi[G]$ is a subgroup of G' and φ is an isomorphism of G with $\varphi[G]$.

Proof. We use Theorem 5.14. Let $x', y' \in \varphi[G]$. Then for for some $x, y \in G$ we have $x' = \varphi(x)$ and $y' = \varphi(y)$. So $x, y \in G$ and so $x'y' = \varphi(x)\varphi(y) = \varphi(xy)$ (by hypothesis), and so $x'y' \in \varphi[G]$. That is, $\varphi[G]$ is closed under the binary operation of G'.

For e' the identity of G', we have $e'\varphi(e) = \varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$ where e is the identity of G. By right cancellation in G', we have $e' = \varphi(e)$ and so $e' \in \varphi[G]$.

Lemma 8.15.

Lemma 8.15. Let G and G' be groups and let $\varphi : G \to G'$ be a one-to-one function such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$. then $\varphi[G]$ is a subgroup of G' and φ is an isomorphism of G with $\varphi[G]$.

Proof. We use Theorem 5.14. Let $x', y' \in \varphi[G]$. Then for for some $x, y \in G$ we have $x' = \varphi(x)$ and $y' = \varphi(y)$. So $x, y \in G$ and so $x'y' = \varphi(x)\varphi(y) = \varphi(xy)$ (by hypothesis), and so $x'y' \in \varphi[G]$. That is, $\varphi[G]$ is closed under the binary operation of G'.

For e' the identity of G', we have $e'\varphi(e) = \varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$ where e is the identity of G. By right cancellation in G', we have $e' = \varphi(e)$ and so $e' \in \varphi[G]$.

Lemma 8.15 (continued).

Lemma 8.15. Let G and G' be groups and let $\varphi : G \to G'$ be a one-to-one function such that $\varphi(xy) = \varepsilon$

Proof (continued). For $x' \in \varphi[G]$ where $x' = \varphi(x)$, we have

$$e' = \varphi(e) = \varphi\left(xx^{-1}\right) = \varphi(x)\varphi\left(x^{-1}\right) = x'\varphi\left(x^{-1}\right),$$

so $(x')^{-1} = \varphi\left(x^{-1}\right) \in \varphi[G]$. So, by Theorem 5.14, $\varphi[G]$ is a subgroup of G'.

Finally, φ is one-to-one by hypothesis, φ is onto $\varphi[G]$ by the definition of $\varphi[G]$, and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$ by hypothesis. So φ is an isomorphism between G and $\varphi[G]$. □

Lemma 8.15 (continued).

Lemma 8.15. Let G and G' be groups and let $\varphi : G \to G'$ be a one-to-one function such that $\varphi(xy) = \varepsilon$

Proof (continued). For $x' \in \varphi[G]$ where $x' = \varphi(x)$, we have

$$e' = \varphi(e) = \varphi\left(xx^{-1}\right) = \varphi(x)\varphi\left(x^{-1}\right) = x'\varphi\left(x^{-1}\right),$$

so $(x')^{-1} = \varphi\left(x^{-1}\right) \in \varphi[G]$. So, by Theorem 5.14, $\varphi[G]$ is a subgroup of G'.

Finally, φ is one-to-one by hypothesis, φ is onto $\varphi[G]$ by the definition of $\varphi[G]$, and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$ by hypothesis. So φ is an isomorphism between G and $\varphi[G]$. □

Theorem 8.16. Cayley's Theorem

Theorem 8.16. Cayley's Theorem Every group is isomorphic to a group of permutations.

Proof. Let G be a group. By Lemma 8.15 we need only find a one-to-one function $\varphi : G \to S_G$ (the group of all permutations on group G) such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$. Then we know that $\varphi[G]$ is a subgroup of the group of permutations S_G. For $x \in G$, define $\lambda_x : G \to G$ as $\lambda_x(g) = xg$ for all $g \in G$. For $c \in G$, we have $\lambda_x(x^{-1}c) = x(x^{-1}c) = c$ and so λ_x is onto G. If $\lambda_x(a) = \lambda_x(b)$, then $xa = xb$ and by left cancellation $a = b$. So λ_x is one-to-one. Therefore λ_x is a permutation of G and so $\lambda_x \in S_G$ for all $x \in G$.

Theorem 8.16. Cayley's Theorem

Theorem 8.16. Cayley's Theorem Every group is isomorphic to a group of permutations.

Proof. Let G be a group. By Lemma 8.15 we need only find a one-to-one function $\varphi : G \to S_G$ (the group of all permutations on group G) such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$. Then we know that $\varphi[G]$ is a subgroup of the group of permutations S_G. For $x \in G$, define $\lambda_x : G \to G$ as $\lambda_x(g) = xg$ for all $g \in G$. For $c \in G$, we have $\lambda_x\left(x^{-1}c\right) = x\left(x^{-1}c\right) = c$ and so λ_x is onto G. If $\lambda_x(a) = \lambda_x(b)$, then $xa = xb$ and by left cancellation $a = b$. So λ_x is one-to-one. Therefore λ_x is a permutation of G and so $\lambda_x \in S_G$ for all $x \in G$.

Define $\varphi : G \to S_G$ as $\varphi(x) = \lambda_x$ for all $x \in G$. Suppose $\varphi(x) = \varphi(y)$. Then $\lambda_x = \lambda_y$, and for $e \in G$ we get $\lambda_x(e) = \lambda_y(e)$ or $xe = ye$ or $x = y$. So φ is one-to-one.

Theorem 8.16. Cayley's Theorem

Theorem 8.16. Cayley's Theorem Every group is isomorphic to a group of permutations.

Proof. Let G be a group. By Lemma 8.15 we need only find a one-to-one function $\varphi : G \to S_G$ (the group of all permutations on group G) such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$. Then we know that $\varphi[G]$ is a subgroup of the group of permutations S_G. For $x \in G$, define $\lambda_x : G \to G$ as $\lambda_x(g) = xg$ for all $g \in G$. For $c \in G$, we have $\lambda_x\left(x^{-1}c\right) = x\left(x^{-1}c\right) = c$ and so λ_x is onto G. If $\lambda_x(a) = \lambda_x(b)$, then $xa = xb$ and by left cancellation $a = b$. So λ_x is one-to-one. Therefore λ_x is a permutation of G and so $\lambda_x \in S_G$ for all $x \in G$.

Define $\varphi : G \to S_G$ as $\varphi(x) = \lambda_x$ for all $x \in G$. Suppose $\varphi(x) = \varphi(y)$. Then $\lambda_x = \lambda_y$, and for $e \in G$ we get $\lambda_x(e) = \lambda_y(e)$ or $xe = ye$ or $x = y$. So φ is one-to-one.

Theorem 8.16. Cayley's Theorem (continued)

Theorem 8.16. Cayley's Theorem (continued) Every group is isomorphic to a group of permutations.

Proof (continued). Next, for any $g \in G$ we have

$$\lambda_{xy}(g) = (xy)\, g = x\,(yg) = x\lambda_y(g) = \lambda_x(\lambda_y(g)) = (\lambda_x \circ \lambda_y)(g)\,.$$

Therefore $\lambda_x \circ \lambda_y = \lambda_x\lambda_y = \lambda_{xy}$ and so $\varphi(x)\,\varphi(y) = \varphi(xy)$. By Lemma 8.15, φ is an isomorphism between group G and group $\varphi[G]$, where $\varphi[G]$ is some subgroup of S_G. That is, G is isomorphic to some group of permutations. □