Introduction to Modern Algebra

Part Part II. Permutations, Cosets, and Direct Products

II.10. Cosets and the Theorem of Lagrange

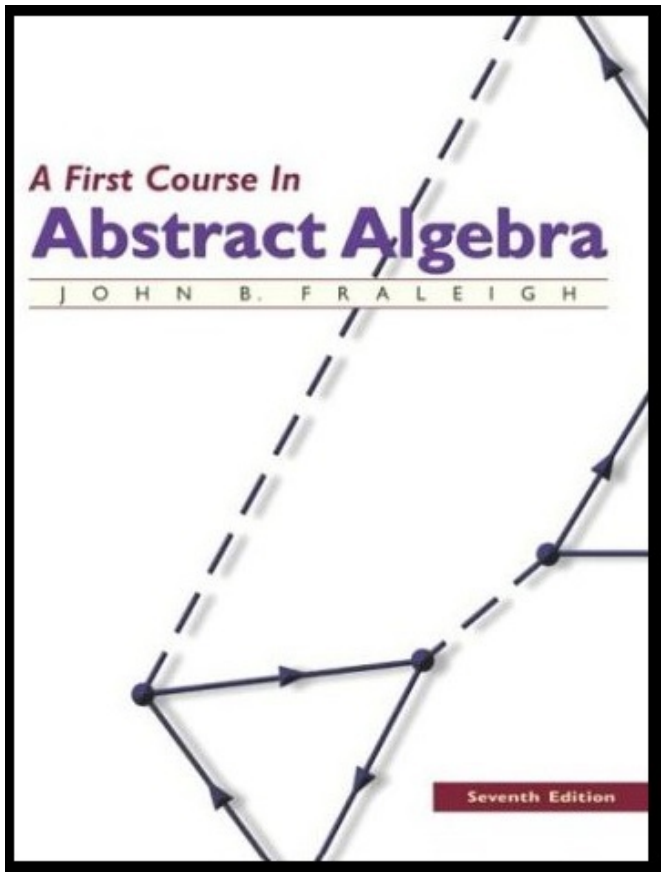

Table of contents

1. Theorem 10.1
2. Lemma
3. Theorem 10.10 (Theorem of Lagrange)
4. Corollary 10.11.
5. Theorem 10.12

Theorem 10.1

Theorem. 10.1. Let H be a subgroup of group G. Let the relation $\sim_L$ be defined on G by $a \sim_L b$ iff $a^{-1}b \in H$. Let $\sim_L$ and $\sim_R$ be defined by $a \sim_R b$ iff $ab^{-1} \in H$. Let $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Proof. We give a proof for $\sim_L$. The proof for $\sim_R$ is similar and is Exercise 10.26. Let $a \in G$. The $a^{-1}a = e$ and $e \in H$ since H is a group. So $a \sim_L a$ and $\sim_L$ is reflexive.

Theorem 10.1

Theorem. 10.1. Let H be a subgroup of group G. Let the relation $\sim_L$ be defined on G by $a \sim_L b$ iff $a^{-1}b \in H$. Let $\sim_L$ and $\sim_R$ be defined by $a \sim_R b$ iff $ab^{-1} \in H$. Let $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Proof. We give a proof for $\sim_L$. The proof for $\sim_R$ is similar and is Exercise 10.26. Let $a \in G$. The $a^{-1}a = e$ and $e \in H$ since H is a group. So $a \sim_L a$ and $\sim_L$ is reflexive.

Suppose $a \sim_L b$. Then $a^{-1}b \in H$. Since H is a group, $\left(a^{-1}b\right)^{-1} = b^{-1}a \in H$ and $b \sim_L a$. So $\sim_L$ is symmetric.

Theorem 10.1

Theorem. 10.1. Let H be a subgroup of group G. Let the relation $\sim_L$ be defined on G by $a \sim_L b$ iff $a^{-1}b \in H$. Let $\sim_L$ and $\sim_R$ be defined by $a \sim_R b$ iff $ab^{-1} \in H$. Let $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Proof. We give a proof for $\sim_L$. The proof for $\sim_R$ is similar and is Exercise 10.26. Let $a \in G$. The $a^{-1}a = e$ and $e \in H$ since H is a group. So $a \sim_L a$ and $\sim_L$ is reflexive.

Suppose $a \sim_L b$. Then $a^{-1}b \in H$. Since H is a group, $\left(a^{-1}b\right)^{-1} = b^{-1}a \in H$ and $b \sim_L a$. So $\sim_L$ is symmetric.

Let $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b, b^{-1}c \in H$. Since H is a group, $\left(a^{-1}b\right)\left(b^{-1}c\right) = a^{-1}c \in H$ and so $a \sim_L c$ and $\sim_L$ is transitive. □

Theorem 10.1

Theorem. 10.1. Let H be a subgroup of group G. Let the relation $\sim_L$ be defined on G by $a \sim_L b$ iff $a^{-1}b \in H$. Let $\sim_L$ and $\sim_R$ be defined by $a \sim_R b$ iff $ab^{-1} \in H$. Let $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Proof. We give a proof for $\sim_L$. The proof for $\sim_R$ is similar and is Exercise 10.26. Let $a \in G$. The $a^{-1}a = e$ and $e \in H$ since H is a group. So $a \sim_L a$ and $\sim_L$ is reflexive.

Suppose $a \sim_L b$. Then $a^{-1}b \in H$. Since H is a group, $\left(a^{-1}b\right)^{-1} = b^{-1}a \in H$ and $b \sim_L a$. So $\sim_L$ is symmetric.

Let $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b, b^{-1}c \in H$. Since H is a group, $\left(a^{-1}b\right)\left(b^{-1}c\right) = a^{-1}c \in H$ and so $a \sim_L c$ and $\sim_L$ is transitive. □

Lemma

Lemma. Consider group G with subgroup H. Then every left coset of H and every right coset of H have the same cardinality, namely $|H|$. That is, for any coset g_1H or Hg_2, there are one-to-one and onto mappings ϕ_1 and ϕ_2 such that $\phi_1 : H \to g_1H$ and $\phi_2 : H \to Hg_2$.

Proof. For $g_1 \in G$, define $\varphi_1 : H \to g_1H$ as $\varphi_1(h) = g_1h$ for each $h \in H$. So (as a set mapping), $\varphi_1(H) = g_1H$ and φ is onto. Next, let $h, h' \in H$ and suppose $\varphi_1(h) = \varphi_1(h')$. That is, suppose $g_1h = g_1h'$. Then by left cancellation in G, $h = h'$ and so φ is one-to-one. The proof for $\varphi_2 : H \to Hg_2$ is similar (it is Exercise 10.27). □

Lemma

Lemma. Consider group G with subgroup H. Then every left coset of H and every right coset of H have the same cardinality, namely $|H|$. That is, for any coset g_1H or Hg_2, there are one-to-one and onto mappings ϕ_1 and ϕ_2 such that $\phi_1 : H \to g_1H$ and $\phi_2 : H \to Hg_2$.

Proof. For $g_1 \in G$, define $\varphi_1 : H \to g_1H$ as $\varphi_1(h) = g_1h$ for each $h \in H$. So (as a set mapping), $\varphi_1(H) = g_1H$ and φ is onto. Next, let $h, h' \in H$ and suppose $\varphi_1(h) = \varphi_1(h')$. That is, suppose $g_1h = g_1h'$. Then by left cancellation in G, $h = h'$ and so φ is one-to-one. The proof for $\varphi_2 : H \to Hg_2$ is similar (it is Exercise 10.27). □

Theorem 10.10 (Theorem of Lagrange)

Theorem 10.10. Theorem of Lagrange ("Lagrange's Theorem"). Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Proof. Suppose $|G| = n$ and $|H| = m$. By Theorem 10.1, the left cosets of H partition G. Let r be the number of left cosets of H. Then, since all left cosets are the same size by "Lemma," $n = mr$ and so $m \mid n$. □

Theorem 10.10 (Theorem of Lagrange)

Theorem 10.10. Theorem of Lagrange ("Lagrange's Theorem"). Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Proof. Suppose $|G| = n$ and $|H| = m$. By Theorem 10.1, the left cosets of H partition G. Let r be the number of left cosets of H. Then, since all left cosets are the same size by "Lemma," $n = mr$ and so $m \mid n$. □

Corollary 10.11.

Corollary 10.11. Every group of prime order is cyclic.

Proof. Let a be an element of group G of prime order p, where a is not the identity of G (recall that 1 is not prime). Then by Theorem 5.17, $\langle a \rangle$ is a subgroup of G. By Lagrange's Theorem (Theorem 10.10), the order of $\langle a \rangle$ divides the order p of G.

Corollary 10.11.

Corollary 10.11. Every group of prime order is cyclic.

Proof. Let a be an element of group G of prime order p, where a is not the identity of G (recall that 1 is not prime). Then by Theorem 5.17, $\langle a \rangle$ is a subgroup of G. By Lagrange's Theorem (Theorem 10.10), the order of $\langle a \rangle$ divides the order p of G. But since p is prime, so the order of $\langle a \rangle$ must be either 1 or p. Since a is not the identity of G, then the order of $\langle a \rangle$ is not 1. So the order of $\langle a \rangle$ is p and $\langle a \rangle = G$. Therefore G is cyclic. □

Corollary 10.11.

Corollary 10.11. Every group of prime order is cyclic.

Proof. Let a be an element of group G of prime order p, where a is not the identity of G (recall that 1 is not prime). Then by Theorem 5.17, $\langle a \rangle$ is a subgroup of G. By Lagrange's Theorem (Theorem 10.10), the order of $\langle a \rangle$ divides the order p of G. But since p is prime, so the order of $\langle a \rangle$ must be either 1 or p. Since a is not the identity of G, then the order of $\langle a \rangle$ is not 1. So the order of $\langle a \rangle$ is p and $\langle a \rangle = G$. Therefore G is cyclic. □

Theorem 10.12

Theorem 10.12. The order of an element of a finite group divides the order of the group.

Proof. The order of $a \in G$ is $|\langle a \rangle|$ by definition, and by Lagrange's Theorem, $|\langle a \rangle| \mid |G|$, since $\langle a \rangle$ is a subgroup of G. □

Theorem 10.12

Theorem 10.12. The order of an element of a finite group divides the order of the group.

Proof. The order of $a \in G$ is $|\langle a \rangle|$ by definition, and by Lagrange's Theorem, $|\langle a \rangle| \mid |G|$, since $\langle a \rangle$ is a subgroup of G. □