Chapter 5. Cosets, Normal Subgroups, and Quotient Groups

5.1 Definition: Let G be a group with operation $*$, let $H \leq G$ and let $a \in G$. The **left coset** of H in G containing a is the set

$$a * H = \{ax | x \in H\}.$$

Similarly the **right coset** of H in G containing a is the set $H * a = \{xa | x \in H\}$. Usually, unless the operation is addition, we write $a * H$ as aH and we write $H * a$ as Ha. We denote the set of left cosets of H in G by G/H so we have

$$G/H = \{aH | a \in G\}.$$

The **index** of H in G, denoted by $[G : H]$ is the cardinality of the set of cosets, that is

$$[G : H] = |G/H|.$$

When G is abelian there is no difference between left and right cosets so we simply call them cosets.

5.2 Example: In the group $\mathbb{Z}_{12}$, the cosets of $H = \langle 3 \rangle = \{0, 4, 8\}$ are

$$\begin{aligned} 0 + H = 4 + H = 8 + H &= \{0, 4, 8\} = H \\ 1 + H = 5 + H = 9 + H &= \{1, 5, 9\} \\ 2 + H = 6 + H = 10 + H &= \{2, 6, 10\} \\ 3 + H = 7 + H = 11 + H &= \{3, 7, 11\} \end{aligned}$$

5.3 Example: In the group $\mathbb{Z}$, for $n \in \mathbb{Z}^+$, the cosets of $\langle n \rangle = n\mathbb{Z}$ are

$$k + n\mathbb{Z} = \{ \cdots, k - 2n, k - n, k, k + n, k + 2n, \cdots \} \text{ where } k \in \mathbb{Z}.$$

These are exactly the elements of $\mathbb{Z}_n$, so we have $\mathbb{Z}/\langle n \rangle = \mathbb{Z}_n$.

5.4 Theorem: *Let G be a group, let $H \leq G$, and let $a, b \in G$. Then*
(1) $b \in aH \iff a^{-1}b \in H \iff aH = bH$,
(2) either $aH = bH$ or $aH \cap bH = \emptyset$, and
(3) $|aH| = |H|$.

Analogous results hold for right cosets.

Proof: If $b \in aH$, say $b = ah$ with $h \in H$, then $a^{-1}b = h \in H$. Conversely if $a^{-1}b \in H$ then $b = ah \in aH$. Thus we have $b \in aH \iff a^{-1}b \in H$. Now suppose that $b \in aH$, say $b = ah$ with $h \in H$. Let $x \in aH$, say $x = ak$ with $k \in H$. Then $x = ak = bh^{-1}k \in bH$. Thus $aH \subseteq bH$. Let $y \in bH$, say $y = bl$ with $l \in H$. Then $y = bl = ahl \in aH$. Thus $bH \subseteq aH$. Conversely, suppose that $aH = bH$. Then $b = be \in bH = aH$. This completes the proof of (1).

To prove (2), suppose that $aH \cap bH \neq \emptyset$. Choose $x \in aH \cap bH$, say $x = ah = bl$ with $h, l \in H$. Then $a^{-1}b = hl^{-1} \in H$ so $aH = bH$ by (1).

To prove (3), define $\phi : H \to aH$ by $\phi(h) = ah$. Then ϕ is clearly surjective, and ϕ is injective since if $\phi(h) = \phi(k)$ then $ah = ak$ and so $h = k$ by cancellation.

5.5 Corollary: (*Lagrange's Theorem*) *Let G be a group and let $H \leq G$. Then*

$$|G| = |G/H|\,|H|\,.$$

Proof: The above theorem shows that the group G is partitioned into left cosets and that these cosets all have the same cardinality.

5.6 Corollary: *Let G be a finite group, let $H \leq G$ and let $a \in G$. Then $|H|$ divides $|G|$ and $|a|$ divides $|G|$.*

5.7 Corollary: (*The Euler-Fermat Theorem*) *For $a \in U_n$ we have $a^{\varphi(n)} = 1$.*

5.8 Corollary: (*The Classification of Groups of Order p*) *Let p be prime. Let G be a group with $|G| = p$. Then $G \cong \mathbb{Z}_p$.*

Proof: Let $a \in \mathbb{Z}_p$ with $a \neq e$. Since $|a|$ divides $|G| = p$ we have $|a| = 1$ or $|a| = p$. Since $a \neq e$, $|a| \neq 1$ so $|a| = p$. Since $\langle a \rangle = |a| = p = |G|$ and $\langle a \rangle \subseteq G$ we have $\langle a \rangle = G$ and so $G = \langle a \rangle \cong \mathbb{Z}_p$.

5.9 Theorem: *Let G be a group and let $H \leq G$. The following are equivalent.*
(1) we can define a binary operation $*$ on G/H by $(aH) * (bH) = (ab)H$,
(2) $aha^{-1} \in H$ for all $a \in G$, $h \in H$, and
(3) $aH = Ha$ for all $a \in H$.
(4) $aHa^{-1} = H$ for all $a \in H$.
In this case, G/H is a group under the above operation $*$ with identity $eH = H$.

Proof: Suppose that we can define an operation $*$ on G/H by $(aH) * (bH) = (ab)H$. The fact that this operation is well-defined means that for all $a_1, a_2, b_1, b_2 \in G$, if $a_1H = a_2H$ and $b_1H = b_2H$ then $(a_1b_1)H = (a_2b_2)H$, or equivalently if $a_1^{-1}a_2 \in H$ and ${b_1}^{-1}b_2 \in H$ then $(a_1b_1)^{-1}(a_2b_2) \in H$, that is ${b_1}^{-1}{a_1}^{-1}a_2b_2 \in H$. For ${a_1}^{-1}a_2 = h \in H$ and ${b_1}^{-1}b_2 = k \in H$, we have ${b_1}^{-1}{a_1}^{-1}a_2b_2 = {b_1}^{-1}h\,b_2 = {b_1}^{-1}b_2{b_2}^{-1}k\,b_2 = k{b_2}^{-1}h\,b_2$, and this lies in H if and only if ${b_2}^{-1}h\,b_2 \in H$. This proves that (1) $\iff$ (2).

Suppose that (2) holds. Let $x \in aH$, say $x = ah$ with $h \in H$. Then $x = ah = aha^{-1}a \in Ha$ since $aha^{-1} \in H$. Thus $aH \subseteq Ha$. Now let $y \in Ha$, say $y = ka$ with $k \in H$. Then $y = ka = aa^{-1}ka \in aH$ since $a^{-1}ka \in H$ by (2). Thus $Ha \subseteq Ha$. This proves that (2) $\Longrightarrow$ (3).

Conversely, suppose that (3) holds. Let $a \in G$ and $h \in H$. Then $ah \in aH = Ha$ so we can choose $k \in H$ so that $ah = ka$. Then we have $aha^{-1} = kaa^{-1} = k \in H$. This proves that (3) $\Longrightarrow$ (2).

The proof that (3) $\iff$ (4) is left as an exercise.

Now suppose that (1) holds and let $*$ be the above operation. We claim that G/H is a group. Indeed, the operation $*$ is associative since

$$\big((aH)*(bH)\big)*(cH) = \big((ab)H\big)*(cH) = (abc)H = (aH)*\big((bc)H\big) = (aH)*\big((bH)*(cH)\big)\,,$$

the coset $eH = H$ is the identity for G/H since for $a \in G$ we have

$$(aH) * (eH) = (ae)H = aH \quad\text{and}\quad (eH) * (aH) = (ea)H = aH\,,$$

and for $a \in G$, the inverse of the coset aH is the coset $a^{-1}H$ since

$$(aH) * (a^{-1}H) = (a\,a^{-1})H = eH \quad\text{and}\quad (a^{-1}H) * (aH) = (a^{-1}a)H = eH\,.$$

5.10 Definition: Let G be a group and let $H \leq G$. If H satisfies the equivalent conditions of the above theorem, then we say that H is a **normal** subgroup of G and we write $H \trianglelefteq G$. When $H \trianglelefteq G$, the group G/H is called the **quotient group** of G by H.

5.11 Theorem: (*The First Isomorphism Theorem*)
(1) if $\phi : G \to H$ is a group homomorphism and $K = \text{Ker}(\phi)$ then $K \trianglelefteq G$ and $G/K \cong \phi(G)$, indeed the map $\Phi : G/K \to \phi(G)$ given by $\Phi(aK) = \phi(a)$ is a group isomorphism.
(2) if $K \trianglelefteq G$ then the map $\phi : G \to G/K$ given by $\phi(a) = aK$ is a group homomorphism with $\text{Ker}(\phi) = K$.

Proof: To prove (1), let $\phi : G \to H$ be a group homomorphism and let $K = \text{Ker}(\phi)$. Let $a \in G$ let $k \in K$ so $\phi(k) = e$. Then $\phi(aka^{-1}) = \phi(a)\phi(k)\phi(a^{-1}) = \phi(a)\phi(a)^{-1} = e$ and so $aka^{-1} \in \text{Ker}(\phi) = K$. This shows that $K \trianglelefteq G$. Define $\Phi : G/H \to \phi(G)$ by $\Phi(aK) = \phi(a)$. Note that Φ is well-defined since if $aK = bK$ then $a^{-1}b \in K$ so we have $\phi(a)^{-1}\phi(b) = \phi(a^{-1}b) = e$ and hence $\phi(a) = \phi(b)$. Note that Φ is a group homomorphism since $\Phi\big((aK)(bK)\big) = \Phi\big((ab)K\big) = \phi(ab)\phi(a)\phi(b) = \Phi(aK)\Phi(bK)$. Finally note that Φ is clearly onto, and Φ is 1:1 since if $\Phi(aK) = e$ then $\phi(a) = e$ so $a \in K$ and hence $aK = K$, which is the identity element of G/K.

To prove (2) let $K \trianglelefteq G$. Define $\phi : G \to G/K$ by $\phi(a) = aK$. Then ϕ is a group homomorphism since $\phi(ab) = (ab)K = (aK)(bK) = \phi(a)\phi(b)$, and $\text{Ker}(\phi) = K$ since for $a \in G$ we have $a \in \text{Ker}(\phi) \iff \phi(a) = eK \iff aK = eK \iff a \in eK = K$.

5.12 Theorem: (*The Second Isomorphism Theorem*) *Let G be a group, let $H \leq G$ and let $K \trianglelefteq G$. Then $K \cap H \trianglelefteq H$, $KH = \langle K \cup H \rangle$, and $H\big/(K \cap H) \cong KH\big/N$.*

Proof: The proof is left as an exercise.

5.13 Theorem: (*The Third Isomorphism Theorem*) *Let G be a group and let $H, K \trianglelefteq G$ with $K \leq H$. Then $H/K \trianglelefteq G/K$ and $(G/K)\big/(H/K) \cong G/H$.*

Proof: The proof is left as an exercise.

5.14 Example: The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(k) = k$ is a group homomorphism with $\text{Image}(\phi) = \langle n \rangle$ and $\text{Ker}(\phi) = \langle n \rangle$, and we have $\mathbb{Z}\big/\langle n \rangle \cong \mathbb{Z}_n$.

5.15 Example: The map $\phi : \mathbb{R} \to \text{S}^1$ given by $\phi(t) = e^{i\,2\pi t}$ is a group homomorphism, since $e^{i\,2\pi(s+t)} = e^{i\,2\pi s}e^{i\,2\pi t}$, with $\text{Image}(\phi) = \text{S}^1$ and $\text{Ker}(\phi) = \mathbb{Z}$ and we have $\mathbb{R}\big/\mathbb{Z} \cong \text{S}^1$.

5.16 Example: The map $\phi : \mathbb{C}^* \to \mathbb{R}^+$ given by $\phi(z) = \|z\|$ is a group homomoprphism, since $\|zw\| = \|z\|\,\|w\|$, with $\text{Image}(\phi) = \mathbb{R}^+$ and $\text{Ker}(\phi) = \text{S}^1$ so we have $\mathbb{C}^*\big/\text{S}^1 \cong \mathbb{R}^+$.

5.17 Example: The map $\phi : \mathbb{C}^* \to \text{S}^1$ given by $\phi(z) = \frac{z}{\|z\|}$, is a group homomorphism, since $\frac{zw}{\|zw\|} = \frac{z}{\|z\|}\frac{w}{\|w\|}$, with $\text{Image}(\phi) = \text{S}^1$ and $\text{Ker}(\phi) = \mathbb{R}^+$ and so $\mathbb{C}^*\big/\mathbb{R}^+ \cong \text{S}^1$.

5.18 Example: For a commutative ring R, the determinant map $\phi : GL_n(R) \to R^*$ given by $\phi(A) = \det(A)$ is a group homomorphism, since $\det(AB) = \det(A)\det(B)$, and it is surjective since for $a \in R^*$ we have $A = \text{diag}(a, 1, \cdots, 1) \in GL_n(R)$ and $\det(A) = a$, and we have $\text{Ker}(\phi) = \big\{A \in GL_n(R)\big|\det(A) = 1\big\} = SL_n(R)$, and so $SL_n(R) \trianglelefteq GL_n(R)$ with $GL_n(R)\big/SL_n(R) \cong R^*$.

5.19 Example: For $n \geq 2$, the map $\phi : S_n \to \mathbb{Z}^* = \{\pm 1\}$ given by $\phi(\alpha) = (-1)^\alpha$ is a group homomorphism since $(-1)^{\alpha\beta} = (-1)^\alpha(-1)^\beta$, and it is surjective since $(-1)^e = 1$ and $(-1)^{(12)} = 1$, and we have $\text{Ker}(\phi) = \big\{\alpha \in S_n\big|(-1)^\alpha = 1\big\} = A_n$, and so $A_n \trianglelefteq S_n$ with $S_n\big/A_n \cong \mathbb{Z}^* = \{\pm 1\}$.

5.20 Example: Let $H = \big\langle (6,2), (3,6) \big\rangle \leq \mathbb{Z}^2$. As an exercise, show that $\big|\mathbb{Z}^2/H\big| = 30$ and that $\mathbb{Z}^2/H$ is cyclic, then find a subjective group homomorphism $\phi : \mathbb{Z}^2 \to \mathbb{Z}_{30}$ with $\text{Ker}(\phi) = H$.

5.21 Example: The map $\phi : G \to \mathrm{Aut}(G)$ given by $\phi(a) = C_a$ (where C_a is conjugation by a, given by $C_a(x) = axa^{-1}$) is a group homomorphism since $C_{ab} = C_a C_b$, and we have $\mathrm{Image}(\phi) = \left\{ C_a \middle| a \in G \right\} = \mathrm{Inn}(G)$ and

$$\begin{aligned}\mathrm{Ker}(\phi) &= \left\{ a \in G \middle| C_a = I \right\} = \left\{ a \in G \middle| axa^{-1} = x \text{ for all } x \in G \right\} \\ &= \left\{ a \in G \middle| ax = xa \text{ for all } x \in G \right\} = Z(G)\end{aligned}$$

and so $Z(G) \trianglelefteq G$ with $G/Z(G) \cong \mathrm{Inn}(G)$.

5.22 Definition: Let $H \leq G$. The **centralizer** of H in G is the set

$$C(H) = C_{\text{G}}(H) = \left\{ a \in G \middle| ax = xa \text{ for all } x \in H \right\}$$

and the **normalizer** of H in G is the set

$$N(H) = N_{\text{G}}(H) = \left\{ a \in G \middle| aH = Ha \right\}.$$

5.23 Theorem: *(The Normalizer/Centralizer Theorem) Let $H \leq G$. Then $C(H) \trianglelefteq N(H)$ and $N(H)/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.*

Proof: The proof is left as an exercise.

5.24 Theorem: *(The Characterization of Internal Direct Products) Let G be a group. Let $H \trianglelefteq G$ and $L \trianglelefteq G$. Suppose that $H \cap K = \{e\}$ and that $G = HK = \left\{ hk \middle| h \in H, k \in K \right\}$. Then $G \cong H \times K$.*

Proof: Define $\phi : H \times K \to G$ by $\phi(h,k) = hk$. The map ϕ is a group homomorphism since for $H_1, h_2 \in H$ and $k_1, k_2 \in K$ we have

$$\begin{aligned}\phi\big((h_1,k_1)(h_2,k_2)\big) &= \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1{k_1}^{-1}h_2k_1{h_2}^{-1}h_2k_2 \\ &= h_1k_1eh_2k_2 = \phi(h_1,k_1)\phi(h_2,k_2),\end{aligned}$$

where we used the fact that the element ${k_1}^{-1}h_2k_1{h_2}^{-1}$ lies in both H and K (it lies in H since $H \trianglelefteq G$ so that ${k_1}^{-1}h_2k_1 \in H$, and it lies in K since $K \trianglelefteq G$ so that $h_2k_1{h_2}^{-1} \in K$), and we have $H \cap K = \{e\}$. The map ϕ is surjective since $G = HK$ so that every element in G is of the form $hk = \phi(h,k)$ for some $h \in H$, $k \in K$, and the map ϕ is injective since for $h \in H$ and $k \in K$ we have $\phi(h,k) = e \Longrightarrow hk = e \Longrightarrow h = k^{-1} \Longrightarrow h,k \in H \cap K \Longrightarrow h = k = e$, since $H \cap K = \{e\}$.

5.25 Theorem: (*The Classification of Groups of Order* $2p$) *Let* p *be prime. Then (up to isomorphism) the distinct groups of order* $2p$ *are* $\mathbb{Z}_{2p}$ *and* D_p.

Proof: Let G be a group with $|G| = 2p$. Suppose that $G \not\cong \mathbb{Z}_{2p}$, so G is not cyclic. By Lagrange's Theorem, each element $a \in G$ has order $|a| = 1, 2, p$ or $2p$. Since G is not cyclic, no element has order $2p$ so every non-identity element in G has order 2 or p.

Suppose first that every non-identity element has order 2. Note that G must be abelian since for all $a, b \in G$ we have $a^2 = b^2 = (ba)^2 = e$ and so $ab = b^2aba^2 = b(ba)^2a = ba$. Fix two distinct non-identity elements $a, b \in G$ and consider the set $H = \{e, a, b, ab\}$. Note that H is closed under the operation and under inversion (since $a^2 = b^2 = e$ and $ab = ba$) and so $H = \langle a, b\rangle \leq G$. By Lagrange's Theorem, we have $|H|\big||G|$, that is $4\big|2p$, and so we must have $p = 2$ and so $|G| = 4 = |H|$, and so $G = H \cong {\mathbb{Z}_2}^2 \cong D_2$.

Now suppose that some non-identity element has order p with $p \neq 2$. Choose $a \in G$ with $|a| = p$. Choose $b \notin \langle a\rangle$. Note that since $\langle a\rangle = p$ and $|G| = 2p$, there are exactly two cosets of $\langle a\rangle$ in G, namely $\langle a\rangle$ and $b\langle a\rangle$, and G is the disjoint union $G = \langle a\rangle \cup b\langle a\rangle$. Note that $b^2\langle a\rangle \neq b\langle a\rangle$ since $b = b^{-1}b^2 \notin \langle a\rangle$, and so we must have $b^2\langle a\rangle = \langle a\rangle$ and hence $b^2 \in \langle a\rangle$. Note that $|b| \neq p$, since if we had $b^p = e$ then (since $p+1$ is even) we would have $b = b^{p+1} \in \langle b^2\rangle \subseteq \langle a\rangle$, and so $|b| = 2$. Similarly, we have $|x| = 2$ for every $x \notin \langle a\rangle$. Consider the element ab. Note that $ab \notin \langle a\rangle = a\langle a\rangle$ since $b = a^{-1}ab \notin \langle a\rangle$, and so we have $|ab| = 2$. Thus $abab = e$ and so $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{p-1}$

We have shown that G is the disjoint union $G = \langle a\rangle \cup b\langle a\rangle$, so we have

$$G = \left\{e, a, a^2, \cdots, a^{p-1}, b, ba, ba^2, \cdots, ba^{p-1}\right\}$$

with the listed elements distinct. Since $ab = ba^{-1}$, we have $a^2b = aba^{-1} = ba^{-2}$ and $a^3b = aba^{-2} = ba^{-3}$ and so on so that $a^kb = ba^{-k}$. This determines the operation on G completely. Indeed we have

$$a^k \cdot a^l = a^{k+l}\ ,\ a^k \cdot ba^l = ba^{l-k}\ ,\ ba^k \cdot a^l = ba^{k+l}\ ,\ ba^k \cdot ba^l = a^{l-k}\,.$$

Compare this to the operation in $D_p = \left\{I, R_1, \cdots, R_{p-1}, F_0, F_1, \cdots, F_{p-1}\right\}$ given by

$$R_k \cdot R_l = R_{k+l}\ ,\ R_k \cdot F_{-l} = F_{-(l-k)}\ ,\ F_{-k}R_l = F_{-(k+l)}\ ,\ F_{-k}F_{-l} = F_{-(l-k)}\,.$$

We see that the map $\phi : G \to D_p$ given by $\phi(a^k) = R_k$ and $\phi(ba^k) = F_k$ is an isomorphism.

5.26 Theorem: (*The Classification of Groups of Order* p^2) *Let* p *be prime. Then (up to isomorphism) the distinct groups of order* p^2 *are* $\mathbb{Z}_{p^2}$ *and* $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof: Let G be a group with $|G| = p^2$. Suppose that $G \not\cong \mathbb{Z}_{p^2}$ so that G is not cyclic. Each $a \in G$ has order $|a| = 1, p$ or p^2. Since G is not cyclic, every non-identity element has order p.

Let a be a non-identity element in G. We claim that $\langle a\rangle \trianglelefteq G$. Suppose, for a contradiction, that $\langle a\rangle \not\trianglelefteq G$. Choose $x \in G$ and $a^k \in \langle a\rangle$ so that $x\,a^k x^{-1} \notin \langle a\rangle$. This implies that $xax^{-1} \notin \langle a\rangle$ since $x\,a^k x^{-1} = (xax^{-1})^k$. Since $xax^{-1} \neq e$ we have $\left|xax^{-1}\right| = p$. Note that $\langle a\rangle \cap \langle\, xax^{-1}\rangle = \{e\}$ because $\langle a\rangle \cap \langle\, xax^{-1}\rangle$ is a proper subgroup of $\langle a\rangle \cong \mathbb{Z}_p$. It follows that the cosets

$$e\langle\, xax^{-1}\rangle, a\langle\, xax^{-1}\rangle, a^2\langle\, xax^{-1}\rangle, \cdots, a^{p-1}\langle\, xax^{-1}\rangle$$

are distinct since if $a^k\langle xax^{-1}\rangle = a^l\langle xax^{-1}\rangle$ then $a^{l-k} \in \langle xax^{-1}\rangle$ so $a^{l-k} \in \langle a\rangle \cap \langle xax^{-1}\rangle$ and hence $a^{l-k} = e$. Thus G is the disjoint union of these p cosets. In particular, the element x^{-1} lies in some coset. But this is not possible since if $x^{-1} \in a^k\langle\, xax^{-1}\rangle$ with say $x^{-1} = a^k x\, a^l x^{-1}$, then we would have $a^k x\, a^l = e$ and hence $x = a^{-k-l} \in \langle a\rangle$. This proves the claim.

Fix a non-identity element $a \in G$ and choose an element $b \in G$ with $b \notin \langle a\rangle$. Then we have $\langle a\rangle \trianglelefteq G$ and $\langle b\rangle \trianglelefteq G$. As above, we have $\langle a\rangle \cap \langle b\rangle = \{e\}$ (since $\langle a\rangle \cap \langle b\rangle$ is a proper subgroup of $\langle a\rangle \cong \mathbb{Z}_p$), and as above this implies that the cosets

$$e\langle b\rangle\,,\ a\langle b\rangle\,,\ a^2\langle b\rangle\,,\ \cdots\,,\ a^{p-1}\langle b\rangle$$

are distinct (since if $a^k\langle b\rangle = a^l\langle b\rangle$ then $a^{l-k} \in \langle b\rangle$ hence $a^{l-k} \in \langle a\rangle \cap \langle b\rangle = \{e\}$). Thus every element of G is of the form $a^i b^j$, that is $G = \langle a\rangle\langle b\rangle$. By the Characterization of Internal Direct Products, we have $G \cong \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

5.27 Definition: A group G is **simple** when its only normal subgroups are $\{e\}$ and G.

5.28 Theorem: F*or* $n \geq 5$, *the alternating group* A_n *is simple.*

Proof: Let $H \trianglelefteq A_n$. We shall show that $H = A_n$. We consider 5 cases. Case 1: suppose first that H contains a 3-cycle, say $(abc) \in H$. Then for any $k \neq a, b, c$ we have $(abk) = (ab)(ck)\,(abc)^2(ck)(ab) \in H$ It follows that $A_n = H$ because A_n is generated by the 3-cycles of the form (abk) with $k \neq a, b$ (as shown in Example 4.25). Case 2: suppose that H contains an element α which, when written in cycle notation, has a cycle of length $r \geq 4$, say $\alpha = (a_1a_2a_3 \cdots a_r)\beta \in H$. Then $(a_1a_3a_r) = \alpha^{-1}(a_1a_2a_3)\alpha(a_1a_2a_3)^{-1} \in H$ and so $H = A_n$ by Case 1. Case 3: suppose that H contains an element α which, when written in cycle notation, has at least two 3-cycles, say $\alpha = (a_1a_2a_3)(a_4a_5a_6)\beta \in H$. Then we have $(a_1a_4a_2a_6a_3) = \alpha^{-1}(a_1a_2a_4)\alpha(a_1a_2a_4)^{-1} \in H$ and so $H = A_n$ by Case 2. Case 4: suppose that H contains an element α which, when written in cycle notation, is a product of one 3-cycle and some 2-cycles, say $\alpha = (a_1a_2a_3)\beta \in H$ where β is a product of disjoint 2-cycles so that $\beta^2 = e$. Then $(a_1a_3a_2) = \alpha^2 \in H$ and so $H = A_n$ by Case 1. Case 5: suppose that H contains an element α which, when written in cycle notation, is a product of 2-cycles, say $\alpha = (a_1a_2)(a_3a_4)\beta \in H$. Then $(a_1a_3)(a_2a_4) = \alpha^{-1}(a_1a_2a_3)\alpha(a_1a_2a_3)^{-1} \in H$. Let $\gamma = (a_1a_3)(a_2a_4)$ and choose b distinct from a_1, a_2, a_3, a_4. Then $(a_1a_3b) = \gamma(a_1a_2b)\gamma(a_1a_3b)^{-1} \in H$ and so $H = A_n$ by Case 1.