Preliminaries

Axiom of Choice Let $(S_i)_{i \in I}$ be an indexed family of non-empty sets. Then there exists a "choice function", i.e. an indexed family $(x_i)_{i \in I}$ such that $x_i \in S_i$

Well Ordering Principle Every set has a well-ordering, i.e. an order s.t. every nonempty subset has a least element.

Zorn's Lemma Let A be a non-empty partially ordered set s.t. every chain in A has an upper bound in A. Then A has a maximal element

Thm AC, well-ordering, and Zorn are all equivalent + independent of ZF.

Ex Thm Every vector space has a basis.

Pf Let V be a vector space. Let C be the collection of all linearly independent subsets of V.

Observe: If $S_1 \subset S_2 \subset S_3 \subset \dots$ is a chain in C, then $\bigcup_{i \in \mathbb{N}} S_i$ is linearly independent, hence ~~[illegible]~~ an upper bound.

Zorn $\Rightarrow$ C has a maximal element $\mathcal{B}$.

Claim $V = \operatorname{span} \mathcal{B}$.

Pf S'pose not: let $v \in V \setminus \operatorname{span} \mathcal{B}$. Then $\mathcal{B} \cup \{v\}$ is linearly independent $\Rightarrow \mathcal{B}$ is not maximal ↯

$\boxtimes$

Chapter 1

Def (i) A <u>semigroup</u> is a set G with an associative operation

(ii) A <u>monoid</u> is a semigroup G with an identity element, i.e. an element $e \in G$ s.t. $ex = xe = x$ for all $x \in G$.

(iii) A <u>group</u> is a monoid G in which every element has an inverse, i.e. for each $x \in G$, there exists $x^{-1} \in G$ s.t. $xx^{-1} = x^{-1}x = e$.

Remark Identity and inverses must be unique

Def A group G is called <u>abelian</u> if the operation is commutative, i.e. $xy = yx$ for all $x, y \in G$.

Ex Classify as semigroup / monoid / group : $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ (under $+$)

$\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Z}\setminus\{0\}$, $\mathbb{Q}$, $\mathbb{Q}\setminus\{0\}$ (under $\cdot$)

Prop 1.3 Let G be a semigroup. Then G is a group iff & only if left* inverses exist and a left* identity exists, i.e.

(i) there exists $e \in G$ s.t. $ex = x$ for all $x \in G$.

(ii) for each $x \in G$, there exists x^{-1} s.t. $x^{-1}x = e$.

Remark Also true for "right".

Ex Dihedral group $D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle$

Symmetries of regular n-gon

Ex Symmetric group

$S_n = \{ \text{bijections of } \{1, \dots, n\} \}$ with composition as operation

Notation 1 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \in S_5$

Notation 2 (cycle notation) $(1\,3\,4\,2) \in S_5$

Ex $(12)(13425) = (1\,3\,4)(2\,5)$

Fact Every element of S_n can be written as a product of disjoint cycles.

—— x ——

Def Let G, H be semigroups (resp. monoids, resp. groups). A homomorphism is a map $f: G \to H$ satisfying $f(ab) = f(a)f(b)$ for all $a, b \in G$.

- If f is injective, it is called a monomorphism*
- If f is surjective, it is called an epimorphism*
- If f is bijective, it is called an isomorphism
- If $f: G \to G$, f is called an endomorphism
- An isomorphism $f: G \to G$ is called an automorphism.

Ex $\det : GL_n(k) \to k^*$ is a homomorphism

Ex If A is an abelian group, the map $a \mapsto a^{-1}$ is an automorphism.
The map $a \mapsto a^2$ is an endomorphism.

Def Let $f: G \to H$ be a homomorphism.

- The Kernel of f is $\operatorname{Ker} f = \{ g \in G \mid f(g) = e \}$
- The image of f is $\operatorname{Im} f = \{ h \in H \mid h = f(g) \text{ for some } g \in G \}$

Ex $\operatorname{Ker} \det = SL_n(k)$

Thm 2.3 Let $f: G \to H$ be a group homomorphism.

(i) f is injective $\iff$ $\text{Ker} f = \{e\}$

(ii) f is ~~an~~ bijective $\iff$ there exists a homomorphism $f^{-1}: H \to G$ s.t. $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$

Def Let G be a group, and $H \subset G$ a subset. If H is a group, then H is called a subgroup and we write $H < G$

Fact If G a group, $H \subset G$ a subset, then H is a subgroup $\iff$ H closed under ~~operation~~. mult + inversion

Ex $\{e\}$, G are always subgroups of G.

Ex $\{1, r, r^2, r^3, \ldots r^{n-1}\}$ is a subgroup of D_n

Cor 2.6 Any intersection of subgroups is a subgroup.

Def Let G be a group, and $X \subset G$ a subset. then
$$\langle X \rangle = \bigcap_{\substack{H_i < G \\ X \subset H_i}} H_i$$
is the subgroup generated by X

Thm 2.8 $\langle X \rangle = \{ a_1^{n_1} a_2^{n_2} \ldots a_t^{n_t} \mid a_i \in X, n_i \in \mathbb{Z} \}$

— x —

Thm Every subgroup of $\mathbb{Z}$ is cyclic.

Thm Every infinite cyclic group is isomorphic to $\mathbb{Z}$. Every finite cyclic group is isomorphic to $\mathbb{Z}_m$.

Thm Let $G = \langle a \rangle$ be a cyclic group. If G is infinite, [illegible] a and a^{-1} are the only generators of G. If $|G| = m$, then $\langle a^k \rangle = G \iff (k, m) = 1$

—— × ——

Recall: Congruence in $\mathbb{Z}$ modulo m (or $\langle m \rangle$)

$a \equiv b \pmod m \iff a-b \equiv 0 \pmod m \iff m \mid a-b \iff a-b \in \langle m \rangle$

<u>Def</u> Let G be a group, $H \leq G$. Let $a, b \in G$.

<u>a is right congruent to b modulo H</u> if $ab^{-1} \in H$

<u>a is left congruent to b modulo H</u> if $a^{-1}b \in H$

<u>Thm 4.2</u> (i) These are equivalence relations

(ii) The equivalence classes are the right (resp. left) cosets $Ha = \{ha \mid h \in H\}$ ...

(iii) $|Ha| = |H| = |aH|$ for all $a \in G$.

<u>Cor 4.3</u> (i+ii) The right (resp left) cosets partition G.

(iii) For all $a, b \in G$ $\quad Ha = Hb \iff ab^{-1} \in H$

$aH = bH \iff a^{-1}b \in H$

(iv) The left and right cosets are in bijection $(Ha \mapsto a^{-1}H)$

<u>Def</u> The index of H in G is the cardinality of the set of distinct cosets denoted $[G:H]$

<u>Ex</u> $[\mathbb{Z} : \langle m \rangle] = m$

<u>Ex</u> $[G:G] = 1 \qquad [G : \langle e \rangle] = |G|$

Thm 4.5 Let $K < H < G$ be groups. Then $[G:K] = [G:H][H:K]$

Pf Write $G = \coprod_{i \in I} Ha_i$ as a partition of right cosets, so $|I| = [G:H]$

$$H = \coprod_{j \in J} Kb_j \qquad \text{so } |J| = [H:K]$$

Then $G = \coprod_{\substack{i \in I \\ j \in J}} Kb_j a_i$ ← Have not shown disjoint yet!

Suppose $Kb_j a_i = Kb_r a_t$, i.e. $b_j a_i = k b_r a_t$ for some $k \in K$.

$$\underbrace{b_j a_i}_{\in\, Ha_i} = \underbrace{k b_r a_t}_{\in\, Ha_t}$$

Since $b_j \in H$ $\qquad$ Since $kb_r \in H$

$\Rightarrow Ha_i = Ha_t \Rightarrow a_i = a_t$

Then $b_j = k b_r$, so $Kb_j = Kb_r \Rightarrow b_j = b_r$. ∎

Cor 4.6 (Lagrange's Theorem) If $H < G$, then $|G| = [G:H]|H|$.
In particular, if G is finite, then $|a| \mid |G|$ for all $a \in G$.

Notation Let G be a group, H, K subsets of G.
$$HK = \{ab \mid a \in H, b \in K\}$$

Remark HK is usually not a subgroup! Even if H, K are subgroups.

Thm 4.7 Let G be a group, and $H, K < G$ be finite. Then $|HK| = \dfrac{|H||K|}{|H \cap K|}$

Pf Let $C = H \cap K$. $C < K$, let $n = [K:C] = \dfrac{|K|}{|C|} = \dfrac{|K|}{|H \cap K|}$ (by Lagrange)

So $K = CK_1 \amalg CK_2 \amalg CK_3 \amalg \dots \amalg CK_n$ for some $K_i \in K$

Claim $HK = HK_1 \amalg HK_2 \amalg \dots \amalg HK_n$

(claim $\Rightarrow |HK| = |H| n = \dfrac{|H||K|}{|H \cap K|}$)

Pf of claim: Need to show

(1) HK_i and HK_j are disjoint

(2) $HK \subset HK_1 \amalg \ldots \amalg HK_n$

(3) $HK \supset HK_1 \amalg \cdots \amalg HK_n$ (immediate)

(1) Suppose $h_i K_i = h_j K_j$

Then $h_j^{-1} h_i = K_j K_i^{-1} \in C$

$\Rightarrow K_j \in CK_i \Rightarrow K_j = K_i$

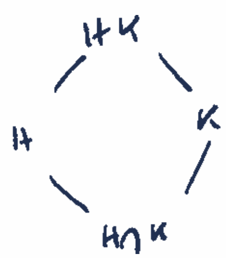
(2) Let $hK \in HK$ $(h \in H,\ K \in K)$

Then $K = cK_i$ for some i, $c \in C$

Then $hK = (hc)K_i \in HK_i$ ☐

Prop 4.8 Let G be a group, $H, K < G$, and suppose HK is a subgroup.

Then $[HK : K] = [H : H \cap K]$ and $[HK : H] = [K : H \cap K]$



hw: $HK = KH$

Pf We will construct bijection $\varphi : \{\text{right cosets of } H\cap K \text{ in } H\} \longrightarrow \{\text{right cosets of } K \text{ in } KH\}$

$$\varphi((H\cap K)h) = Kh$$

well defined: S'pose $(H\cap K)h_1 = (H\cap K)h_2$, i.e. $h_1 h_2^{-1} \in H \cap K < K$, so $Kh_1 = Kh_2$

Surjective: clear

Injective: S'pose $\varphi((H\cap K)h_1) = \varphi((H\cap K)h_2)$

$Kh_1 = Kh_2$

$h_1 h_2^{-1} \in K$, so $h_1 h_2^{-1} \in H\cap K$, so $(H\cap K)h_1 = (H\cap K)h_2$ ☐

Prop 4.9 Let G be a group, $H, K < G$ s.t. HK is a subgroup. If H, K are finite index in HK, then $[HK : H \cap K] = [HK : H][HK : K]$

Pf Thm 4.5 + Prop 4.8 ☐

— x —

Thm 5.1 Let N be a subgroup of a group G. TFAE

(i) Left cosets are right cosets

(ii) $aN = Na$ for all $a \in G$

(iii) $aNa^{-1} = N$ for all $a \in G$.

(iv) N is closed under conjugation by elements of G.

Def If N satisfies these conditions it is called a <u>normal</u> subgroup of G, denoted $N \lhd G$.

Pf (i) $\Rightarrow$ (ii) Let aN be a left coset. Then $aN = Nb$ for some $b \in G$. In particular, $a \in Na \cap Nb \Rightarrow Na = Nb$. So $aN = Na$.

(ii) $\Rightarrow$ (iii) Immediate.

(iii) $\Rightarrow$ (iv) Immediate

(iv) $\Rightarrow$ (i) Let aN be a left coset. If $b \in N$, $aba^{-1} \in N$, so $ab \in Na \Rightarrow aN \subset Na$. Similarly, $Na \subset aN$. ☐

Ex In an abelian group, all subgroups are normal!

Ex Recall $D_4 = \langle r, s \mid r^4 = 1, s^2 = 1, srs = r^{-1} \rangle$

$N = \langle r \rangle = \{1, r, r^2, r^3\}$ is normal

$H = \langle sr \rangle$ is not normal

Remark: If $N \lhd G$ and $N < H < G$, then $N \lhd H$ Caution! $N \lhd K \lhd G$ does <u>not</u> imply $N \lhd G$!

Thm 5.3 Let G be a group, $K < G$, $N \lhd G$

(i) $N \cap K \lhd K$

(ii) $N \lhd \langle N, K \rangle$ (book uses notation $N \vee K$)

(iii) $NK = KN = \langle N, K \rangle$

(iv) If $K \lhd G$ and $K \cap N = \langle e \rangle$, then $nk = kn$ for all $k \in K$, $n \in N$.

Pf (i) Let $x \in N \cap K$, $a \in K$. Then $N \lhd G \Rightarrow axa^{-1} \in N$; $x, a \in K \Rightarrow axa^{-1} \in K$ $\Rightarrow axa^{-1} \in N \cap K$.

(ii) Remark (show if NK a subgroup, $NK = KN$ (homework))

(iii) It suffices to show $\langle N, K \rangle = NK$

Trivial: $NK \subset \langle N, K \rangle$

Let $n_1 k_1 n_2 k_2 \dots n_r k_r \in \langle N, K \rangle$ $(n_i \in N,\ k_i \in K)$

Induct on n: If $r = 1$, $n_1 k_1 \in NK$

If $r > 1$: Assume $n_1 k_1 \dots n_{r-1} k_{r-1} = n_0 k_0 \in NK$

$$n_1 k_1 \dots n_{r-1} k_{r-1} n_r k_r = n_0 k_0 n_r k_r = \underbrace{n_0 (k_0 n_r k_0^{-1})}_{N} \underbrace{k_0 k_r}_{K} \in NK$$

(iv) $\underbrace{n \overbrace{k n^{-1}}}_{K}\overbrace{{}k^{-1}}^{\in N} \in K \cap N = \langle e \rangle$, so $nkn^{-1}k^{-1} = e \Leftrightarrow nk = kn$. ∎

Thm 5.4 Let G be a group, $N \lhd G$. Then G/N (set of cosets of N) is a group of order $[G:N]$ with multiplication $(aN)(bN) = abN$.

Pf Need to show multiplication is well defined, i.e. if $aN = \tilde{a}N$, $bN = \tilde{b}N$, then $abN = \tilde{a}\tilde{b}N$.

write $\tilde{a} = an_1$ $\quad \tilde{b} = bn_2$

Then $\tilde{a}\tilde{b} = an_1bn_2 = ab(b^{-1}n_1b)n_2 \in abN$ ∎

Def G/N is called the quotient group or factor group of G by N.

Ex $\mathbb{Z}$ is abelian, so $\langle m\rangle \lhd \mathbb{Z}$. Then $\mathbb{Z}/\langle m\rangle$ is exactly the group of integers mod m.

Ex $D_4/\langle r\rangle = \{\langle r\rangle, s\langle r\rangle\} \cong \mathbb{Z}/\langle 2\rangle$

Thm 5.5 (i) If $f: G \to H$ is a group hom., then $\ker f \lhd G$.

(ii) If $N \lhd G$, then $\pi: G \to G/N$ is a (surjective) hom with $\ker \pi = N$
$\pi(a) = aN$.

Pf (1) Let $x \in \ker f$, $a \in G$. Want $axa^{-1} \in \ker f$

Compute $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)ef(a)^{-1} = e \quad \Rightarrow axa^{-1} \in \ker f$

(2) Let $a, b \in G$. Want $\pi(ab) = \pi(a)\pi(b)$

$\pi(ab) = abN$ $\qquad$ So π is a homomorphism

$\pi(a)\pi(b) = aNbN = abN$

$\pi(a) = N \Leftrightarrow aN = N \Leftrightarrow a \in N$ ∎

$\ker \pi = \{a \in G \mid \pi(a) = eN = N\}$

Thm 5.6 Let $f: G \to H$ be a homomorphism, $N \trianglelefteq G$. If $N \subset \operatorname{Ker} f$, then there exists a unique homomorphism $\bar{f}: G/N \to H$ such that the diagram commutes

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

Pf Define* $\bar{f}: G/N \to H$ by $\bar{f}(aN) = f(a)$

Careful! Need to check well-defined whenever defining in terms of coset representatives

Need to check: If $aN = bN$, then $\bar{f}(aN) = \bar{f}(bN)$

↳ write $a = bn$ for some $n \in N$.

$\bar{f}(aN) = f(a) = f(bn) = f(b)f(n) = f(b) = \bar{f}(bN)$

since $N < \operatorname{Ker} f$

Is $\bar{f}$ a homomorphism? Let $aN, bN \in G/N$.

$\bar{f}(aN\, bN) = \bar{f}(abN) = f(ab)$

$\bar{f}(aN)\bar{f}(bN) = f(a)\, f(b)$ ″ ∎

Remark $N \trianglelefteq \operatorname{Ker} f$, and $\operatorname{Ker} \bar{f} = \operatorname{Ker} f / N$

Corollary 5.7 (First Isomorphism theorem) If $f: G \to H$ is a group homomorphism, then $G/\operatorname{Ker} f \cong \operatorname{Im} f$

Pf

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d] & \operatorname{Im} f \\ G/\operatorname{Ker} f \arrow[ur, dashed] & \end{tikzcd}$$

Surjective by construction
Injective by remark

∎

Corollary 5.9 (Second Isomorphism Theorem) Let G be a group, $K \leq G$, $N \trianglelefteq G$.
Then $K/N\cap K \cong NK/N$

Pf Let φ be the composition $K \hookrightarrow NK \longrightarrow NK/N$ (so $\varphi(a) = aN$)

$$K \xrightarrow{\varphi} NK/N$$

Claim $\operatorname{Ker}\varphi = N \cap K$
If $a \in N\cap K$, $\varphi(a) = aN = N$ (since $a \in N$), so $a \in \operatorname{Ker}\varphi$
If $a \in \operatorname{Ker}\varphi$, $\varphi(a) = N$, so $a \in N \Rightarrow a \in N \cap K$.

$$\begin{tikzcd} K \arrow[r, "\varphi"] \arrow[d] & NK/N \\ K/N\cap K \arrow[ur, dashed, "\bar{\varphi}"'] & \end{tikzcd}$$

Since $N \cap K = \operatorname{Ker}\varphi$, $\bar{\varphi}$ is injective.
To see φ surjective: Let $aN \in NK/N$
Since $NK = KN$, write $a = kn$ for some $k \in K$, $n \in N$.
Then $aN = knN = kN = \varphi(k)$.

$\Rightarrow \bar{\varphi}$ is an isomorphism. $\square$

Corollary 5.10 (Third Isomorphism Theorem) Let G be a group, $H \trianglelefteq G$, $K \trianglelefteq G$ with $K < H$. Then $H/K \trianglelefteq G/K$ and $G/K\big/H/K \cong G/H$

Pf Let φ be the ~~composition~~ quotient map $G \longrightarrow G/H$

$$\begin{tikzcd} G \arrow[r] \arrow[d] & G/H \\ G/K \arrow[ur, dashed, "\bar{\varphi}"'] & \end{tikzcd}$$

We get a surjective map $\bar{\varphi} : G/K \longrightarrow G/H$
Suppose $aK \in \operatorname{Ker}\bar{\varphi}$, so $\underbrace{\bar{\varphi}(aK)}_{= aH} = H$, iff $a \in H$. Thus $H/K = \operatorname{Ker}\bar{\varphi}$

$\square$

—×—

Thm 6.3 Every element of S_n can be written uniquely* as a product of disjoint cycles

* Can permute the cycles

Corollary 6.4 The order of a permutation is the least common multiple of the orders of its disjoint cycles

Corollary 6.5 Every permutation can be written as a product of transpositions

Pf $(x_1 x_2 \dots x_r) = (x_1 x_r)(x_1 x_{r-1}) \dots (x_1 x_3)(x_1 x_2)$

Caution: Not unique! $(12)(13) = (31)(32)$

Def 6.6 A permutation is **even** (resp **odd**) if it can be written as a product of an even (resp odd) number of transpositions.

Ex $(132) \in S_3$ is even since $(132) = (12)(13)$

(In general: odd length cycles are even)

Thm 6.7 ~~Even~~ A permutation cannot be both even & odd.

Claim If τ_i are transpositions & $\tau_1 \dots \tau_r = id$, then r is even

spose $\sigma_1 \dots \sigma_s = \tau_1 \dots \tau_r$

then $\sigma_1 \dots \sigma_s \tau_r^{-1} \dots \tau_1^{-1} = id$, so $r+s$ is even (i.e. both odd or both even)

Pf of claim Suppose $\tau_1 \dots \tau_r = id$. Induction r

Products of transpositions:

$(ab)(ab) = id$

$(ab)(cd) = (cd)(ab)$

$(ab)(ac) = (bc)(ab)$

$(ab)(bc) = (bc)(ac)$

Push 1's to far right, then 2's, etc. Induct. ∎

Thm 6.8 For $n \geq 2$, let A_n be the set of all even permutations of S_n. Then A_n is a normal subgroup of index 2 (and is the only subgroup of index 2).

Pf Define $\text{sgn} : S_n \longrightarrow \mathbb{Z}_2$ is a homomorphism with kernel A_n.

Exercise It is the only subgroup of index 2 $\blacksquare$

Def A_n is called the **alternating group**

Def A group G is called **simple** if it has no proper normal subgroups

Ex $\mathbb{Z}_p$ for prime p are precisely the simple abelian groups

Thm 6.10 A_n is simple if and only if $n \neq 4$

Lemma $\sigma\,(x_1\, x_2 \dots x_r)\,\sigma^{-1} = (\sigma(x_1)\; \sigma(x_2) \;\dots\; \sigma(x_r))$

Ex Let $\sigma = (1\,2\,3)$

$\sigma\,(1\,5\,2\,3\,4)\,\sigma^{-1} = (2\,5\,3\,1\,4)$

$(1\,2\,3)(1\,5\,2\,3\,4)(3\,2\,1) = (1\,4\,2\,5\,3)$

Lemma If $n \geq 5$, all 3-cycles are conjugate in A_n

Pf By lemma, conjugate in $\underline{\underline{S_n}}$

i.e. If τ_1, τ_2 are 3-cycles $\quad \tau_1 = \sigma \tau_2 \sigma^{-1}$ for some $\sigma \in S_n$

If σ is odd: choose 2 elements a, b not appearing in τ_2

then $\tilde{\sigma} = \sigma(ab)$ is even, and $\tilde{\sigma}\tau_2\tilde{\sigma}^{-1} = \sigma(a\,b)\tau_2(a\,b)\sigma^{-1}$

$= \sigma \tau_2 \sigma^{-1}$

$= \tau_1$ $\blacksquare$

Lemma Let $n \geq 5$. If $N \lhd A_n$ and N contains a 3-cycle, then $N = A_n$

Pf It suffices to show that A_n is generated by 3-cycles

Claim A product of two transpositions is generated by 3-cycles.

Pf **Case 1** $(ab)(cd) = (acb)(acd)$

Case 2 $(ab)(ac) = (acb)$

~~Case~~ **Case 3** $(ab)(ab) = id.$ $\boxtimes$

Pf of Thm 6.10 Suppose $H \lhd A_n$ is nontrivial. We will show H contains a 3-cycle.

Cases: Disjoint cycle structure of elements of H

Case 1 Cycle of length $r \geq 4$

WLOG $\sigma = (1\,2\,3 \ldots r)\tau$

Let $\delta = (1\,2\,3)$

$$H \ni \sigma^{-1}\delta\sigma\delta^{-1} = \tau^{-1}(r \ldots 3\,2\,1)(1\,2\,3)(1\,2\,3 \ldots r)\tau(3\,2\,1)$$

$$= (1\;3\;r)$$

Case 2 Multiple 3-cycles

WLOG $\sigma = (1\,2\,3)(4\,5\,6)\tau$

Let $\delta = (1\,2\,4)$

$$H \ni \sigma^{-1}\delta\sigma\delta^{-1} = \tau^{-1}(6\,5\,4)(3\,2\,1)(1\,2\,4)(1\,2\,3)(4\,5\,6)\tau(4\,2\,1)$$

$$= (1\;4\;2\;6\;3)$$

Apply Case 1

<u>Case 3</u> Single 3-cycle

wLOG $\sigma = (123)\tau$

$N \ni \sigma^2 = (123)\tau(123)\tau = (123)^2\tau^2 = (123)^2 = (123)^{-1} = (321)$

<u>Case 4</u> Product of transpositions

wLOG $\sigma = (12)(34)\tau$

Let $\delta = (123)$

$H \ni \sigma^{-1}\delta\sigma\delta^{-1} = \tau(34)(12)(123)(12)(34)\tau(321)$

$= (13)(24)$

Call this $\sigma_0 \in H$

Let $\delta_0 = (135)$

$\sigma_0^{-1}\delta_0\sigma_0\delta_0^{-1} = (13)(24)(135)(13)(24)(531)$

$= (135)$

$\boxtimes$