# Preliminaries

**Axion 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 $B$.

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

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

$\boxtimes$

## Chapter 1

**Def** (i) A semigroup is a set $G$ with an associative operation

(ii) A monoid 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 group 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 abelian 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 if & 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

$S_n = \{$ 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.

**~~Ex~~ 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 $\iff$ $\operatorname{Ker} f = \{e\}$

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

**Def** Let $G$ be a group, and $H \subset G$ a subset. If $H$ is a group, then $H$ is called a <u>subgroup</u> 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** $\{1, r, r^2, r^3, \dots r^{n-1}\}$ 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 <u>subgroup generated by $X$</u>

**Thm 2.8** $\langle X \rangle = \{ a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \mid a_i \in X, n_i \in \mathbb{Z} \}$

— 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, $a$ 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 $\langle m \rangle$)

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

Def Let $G$ be a group, $H \leq G$. Let $a, b \in G$.

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

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

Thm 4.2 (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 $a \in G$.

Cor 4.3 (i+ii) The right (resp left) cosets partition $G$.

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

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

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

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

Ex $[\mathbb{Z} : \langle m \rangle] = m$

Ex $[G:G] = 1$ $[G : \langle e \rangle] = |G|$

**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 $|I| = [G:H]$

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

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

Suppose $K b_j a_i = K b_r a_t$, i.e. $\underbrace{b_j a_i}_{\substack{\cap \\ Ha_i}} = \underbrace{k b_r a_t}_{\substack{\cap \\ Ha_t}}$ for some $k \in K$.

Since $b_j \in H$ $\qquad$ Since $k b_r \in H$

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

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

**Cor 4.6** (Lagrange's Theorem) If $H < G$, then $|G| = [G:H]\,|H|$.

In particular, if $G$ is finite, then $|a| \,\big|\, |G|$ for all $a \in G$.

**Notation** Let $G$ be a group, $H, K$ [redacted]. 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 $\Rightarrow |HK| = |H|n = \dfrac{|H||K|}{|H \cap K|}$)

<u>Pf of claim</u> Need to show

(1) $HK_i$ and $HK_j$ are disjoint

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

(3) $HK \supset HK_1 \amalg \dots \amalg HK_n$ (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 $hK = (hc)K_i \in HK_i$ $\square$

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

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

$$\begin{tikzcd}[column sep=small] & HK \arrow[dl, dash] \arrow[dr, dash] & \\ H \arrow[dr, dash] & & K \arrow[dl, dash] \\ & H \cap K & \end{tikzcd}$$

hw: $HK = KH$

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

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

<u>well defined</u> 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 $Kh_1 = Kh_2$

<u>Surjective</u> clear

<u>Injective</u> 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 $(H \cap K)h_1 = (H \cap K)h_2$ $\square$

**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 $\square$

— 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, $Na \subset aN$. $\square$

**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 $N \lhd G$!

<u>Thm 5.3</u> 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 $k \in K$, $n \in N$.

<u>Pf</u> (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

(iii) It suffices to show $\langle N, K \rangle = NK$ (show if $NK$ a subgroup, $NK = KN$ (homework))

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

**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 $\mathrm{Ker}\, f \lhd G$.

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

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

Compute $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)\,e\,f(a)^{-1} = e$ $\Rightarrow axa^{-1} \in \mathrm{Ker}\, f$

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

$\pi(ab) = abN$

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

So $\pi$ is a homomorphism

$\mathrm{Ker}\,\pi = \{a \in G \mid \pi(a) = eN = N\}$

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

**Thm 5.6** Let $f: G \to H$ be a homomorphism, $N \lhd G$. 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* $\bar{f}: G/N \longrightarrow H$ 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 $\bar{f}(aN) = \bar{f}(bN)$

$\hookrightarrow$ write $a = bn$ for some $n \in N$.

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

$\uparrow$ Since $N < \operatorname{Ker} f$

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

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

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

$\blacksquare$

**Remark** $N \lhd \operatorname{Ker} f$, 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

$\blacksquare$

**Corollary 5.9** (Second Isomorphism Theorem) Let $G$ be a group, $K \le G$, $N \trianglelefteq G$.

Then $K/N\cap K \cong NK/N$

**Pf** Let $\varphi$ 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 $\varphi$ 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 $\left(G/K\right)/\left(H/K\right) \cong G/H$

**Pf** Let $\varphi$ be the ~~composition~~ quotient map

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

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 $H/K = \operatorname{Ker}\bar{\varphi}$

$\square$

— x —

**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 <u>even</u> (resp <u>odd</u>) 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** A permutation cannot be both even + odd.

**Claim** If $\tau_i$ are transpositions + $\tau_1 \dots \tau_r = id$, then $r$ is even

s'pose $\sigma_1 \dots \sigma_s = \tau_1 \dots \tau_r$

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 $\square$

**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 $\sigma = (123)$

$\sigma (15234) \sigma^{-1} = (25314)$

$(123)(15234)(321) = (14253)$

**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 $\tau_1, \tau_2$ are 3-cycles $\quad \tau_1 = \sigma \tau_2 \sigma^{-1}$ for some $\sigma \in S_n$

If $\sigma$ is odd: choose 2 elements $a, b$ not appearing in $\tau_2$

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

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

$= \tau_1$ $\square$

**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~~ 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

Case 3 Single 3-cycle

WLOG $\sigma = (123)\tau$

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

Case 4 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 $\delta_0 = (135)$

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

$= (135)$

$\boxtimes$

<u>Def</u> Let $G, H$ be groups. The <u>direct product</u> $G \times H$ is the group (or <u>direct sum</u>)

$$G \times H = \{ (g,h) \mid g \in G, h \in H \}$$

with operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

<u>Ex</u> $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{ (0,0), (0,1), (0,2), (1,0), (1,1), (1,2) \}$

$$(1,1) + (0,2) = (1+0, 1+2) = (1,0)$$

<u>Fact</u> $|G \times H| = |G|\,|H|$

<u>Natural homomorphisms</u>

$$\begin{tikzcd} & G \times H \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ G & & H \end{tikzcd}$$

$\pi_1(g,h) = g$

$\pi_2(g,h) = h$

$$\begin{tikzcd} & G \times H & \\ G \arrow[ur, "i_1"] & & H \arrow[ul, "i_2"'] \end{tikzcd}$$

$i_1(g) = (g, e_H)$

$i_2(h) = (e_G, h)$

<u>Observe</u> $\operatorname{Ker} \pi_1 = i_1(G) \cong G$

$\operatorname{Ker} \pi_2 = i_2(H) \cong H$

$G \times H / G \cong H$

$G \times H / H \cong G$

<u>Remark</u> $G \times H$ is generated by $i_1(G)$, $i_2(H)$

<u>Def</u> Let $\{G_i\}_{i \in I}$ be a collection of groups.

Then $\prod_{i \in I} G_i$ is a group called the <u>direct product</u> of $\{G_i\}_{i \in I}$

**Thm 8.2** The direct product is a categorical product.

**Special Case** Let $G_1, G_2$ be groups, and suppose $H$ is a group with $\varphi_1 : H \to G_1$
$\varphi_2 : H \to G_2$.

There exists unique $\varphi : H \to G_1 \times G_2$ s.t. $\pi_i \varphi = \varphi_i$

$$\begin{tikzcd} & H \arrow[dl, "\varphi_1"'] \arrow[dr, "\varphi_2"] \arrow[d, dashed, "\varphi"] & \\ G_1 & G_1 \times G_2 \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & G_2 \end{tikzcd}$$

**Pf** $\varphi = (i_1\varphi_1, i_2\varphi_2)$ $\square$

**Ex** Let $G = \prod_{n \in \mathbb{N}} \mathbb{Z}_2$

Let $H = \langle i_n(\mathbb{Z}) \mid n \in \mathbb{N} \rangle$

$= \langle (1,0,0,\dots), (0,1,0,0,\dots), (0,0,1,0,0,\dots), \dots \rangle$

Does $H = G$ ?

**Def** The <u>direct sum</u> (or <u>weak direct product</u>) is the subgroup of $\prod_{i \in I} G_i$ generated by the $G_i$.

It consists of elements with <u>finitely many</u> terms not equal to the identity.

**Ex** $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}$

$\prod_{i \in \mathbb{N}} \mathbb{Z}$

**Ex** Is $D_4 = \langle r, s \mid r^4 = 1, s=1, srs = r^{-1} \rangle$ a direct product?

$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$N = \langle r \rangle$ $\quad$ $H = \langle s \rangle$

$\uparrow$ Not normal!

Note that $D_4 = \underset{HN}{\overset{\shortparallel}{NH}}$ and $N \cap H = \langle e \rangle$

Every element of $D_4$ can be written uniquely as $hn$ for some $h \in H$, $n \in N$.

**Thm** Let $N \trianglelefteq G$, $H \leq G$. Then TFAE

(1) $G = NH = HN$ and $N \cap H = \langle e \rangle$

(2) Every element of $G$ can be written uniquely as $nh$ for some $n \in N$, $h \in H$.

(3) Every element of $G$ can be written uniquely as ~~hn~~ $hn$ for some $h \in H$, $n \in N$

(4) There exists a split exact sequence

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] & G \arrow[r] & H \arrow[r] \arrow[l, bend left, dashed] & 1 \end{tikzcd}$$

**Def** Such a $G$ is called the semidirect product of $N$ and $H$, written $G = N \rtimes H$.

**Pf** (1) $\Rightarrow$ (2) uniqueness: Suppose $n_1 h_1 = n_2 h_2$ for some $n_1, n_2 \in N$, $h_1, h_2 \in H$

Then $n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H = \langle e \rangle$

Thus $n_2^{-1} n_1 = e$ $\quad$ $h_2 h_1^{-1} = e$

$n_1 = n_2$ $\quad$ $h_1 = h_2$

(2) $\Rightarrow$ (3) $(nh)^{-1} = h^{-1} n^{-1}$

(3) $\Rightarrow$ (4)

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\alpha"] & G \arrow[r, "\beta"] & H \arrow[r] \arrow[l, bend left, dashed, "\sigma"] & 1 \end{tikzcd}$$

$\alpha =$ inclusion (injective) $\quad$ Define $\beta : G \to H$ by $\beta(hn) = h$.

$\sigma =$ inclusion

Is $\beta$ a homomorphism?

Let $h_1n_1, h_2n_2 \in G$ $\quad (h_1,h_2 \in H, n_1,n_2 \in N)$

$\beta(h_1n_1) = h_1 \quad \beta(h_2n_2) = h_2$

$$\beta(h_1n_1h_2n_2) = \beta(h_1h_2 \underbrace{\underbrace{h_2^{-1}n_1h_2}\underbrace{n_2}}_{N}) = h_1h_2 = \beta(h_1n_1)\beta(h_2n_2)$$

Note $\beta$ surjective, and $\beta \circ \sigma = id$. Also $\mathrm{Ker}\,\beta = \mathrm{Im}\,\alpha$

(4)$\Rightarrow$(1) Suppose $1 \to N \xrightarrow{\alpha} G \underset{\sigma}{\overset{\beta}{\rightleftarrows}} H \to 1$ is a split exact sequence.

Let $x \in G$. We want to break it down into a $H$ part and a $N$ part.
$\sigma(H)$ $\alpha(N)$

Set $h = \sigma\beta(x) \in \sigma(H)$

<u>Claim</u> $xh^{-1} \in \mathrm{Ker}\,\beta = \alpha(N)$

(Then $x \in \alpha(N)\sigma(H) \cong NH$)

<u>Pf</u> $\beta(xh^{-1}) = \beta(x\,\sigma\beta(x^{-1}))$

$= \beta(x)\,\beta\sigma\beta(x^{-1})$

$= \beta(x)\beta(x^{-1})$

$= e$

Need to check $\alpha(N) \cap \sigma(H) = \langle e \rangle$.

Let $x \in \alpha(N) \cap \sigma(H)$. Then $x = \sigma(y)$ for some $y \in H$.

Since $x \in \alpha(N)$, $e_H = \beta(x) = \beta\sigma(y) = y$, so $x = \sigma(e) = e$ $\square$

<u>Cor</u> If $G = N \rtimes H$, then $H \cong G/N$

**Def** Let $X$ be a set.

Let $X^{-1}$ be a set disjoint from $X$ with $|X| = |X^{-1}|$

choose a bijection $X \longrightarrow X^{-1}$, and label the image of $x \in X$ by $x^{-1}$.

A *word* on $X$ is a sequence $(a_1, a_2, a_3, \dots)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ that is eventually identically $1$.

The *empty word* is $(1, 1, 1, \dots)$

A word is *reduced* if $a_i$ never equals $a_{i+1}^{-1}$

**Ex** $X = \{x, y\}$

$(x, y, x, x, x^{-1}, y, y, 1, 1, 1, \dots)$ is a word (Think: $xyxxx^{-1}yy$)

$(x, y, x, y, y, 1, 1, 1, \dots)$ is a reduced word (Think: $xyxyy$)

Usually nonempty reduced words are written of form $x_1^{\lambda_1} \cdots x_r^{\lambda_r}$ $\quad \lambda_r \in \mathbb{Z} \setminus \{0\}$, $x_i \in X$

**Def** The set of all reduced words forms a group called the *free group on $X$* denoted $F(X)$

**Thm 9.2** The free group is a free object in the category of groups.

In other words, if $f : X \longrightarrow G$ is a map of sets to a group $G$, there is a unique homomorphism $\tilde{f} : F(X) \to G$

$$\begin{tikzcd} & G \\ X \arrow[ur, "f"] \arrow[r, hook] & F(X) \arrow[u, dashed, "\tilde{f}"'] \end{tikzcd}$$

**Pf** Define $\tilde{f}(x_1^{\lambda_1} \cdots x_r^{\lambda_r}) = f(x_1)^{\lambda_1} \cdots f(x_r)^{\lambda_r}$

**Cor 9.3** Every group is the homomorphic image of a free group.

**Pf** Let $X$ be a set of generators of $G$. (Note: $G \cong F(X)/\ker \tilde{f}$)

$$\begin{tikzcd} & G \\ X \arrow[ur] \arrow[r, hook] & F(X) \arrow[u, "\tilde{f}"'] \end{tikzcd}$$

∎

<u>Thm-Def 1.1</u> Let $F$ be an abelian group. TFAE

(i) $F$ has a nonempty <u>basis</u>, i.e. a generating set $X$ s.t.
whenever $n_1x_1 + \dots + n_kx_k = 0$ for some $n_i \in \mathbb{Z}$, $x_i \in X$, then $n_i = 0$ for all $i$.
(Think: no nontrivial linear combinations make zero $\Rightarrow$ no relations among generators)

(ii) $F$ is the direct sum of a family of infinite cyclic subgroups

(iii) $F$ is the direct sum of copies of $\mathbb{Z}$

(iv) $F$ is free in the category of abelian groups; i.e.
There is a nonempty set $X \hookrightarrow F$ s.t. given any abelian group $G$ with a set map $f: X \to G$, there exists unique $\tilde{f}: F \to G$

$$\begin{tikzcd} & G \\ X \arrow[ur, "f"] \arrow[r, hook] & F \arrow[u, dashed, "\tilde{f}"'] \end{tikzcd}$$

<u>Pf</u> (i) $\Rightarrow$ (ii) If $x \in X$, then $\langle x \rangle$ is infinite (cyclic) group
Need to check: If $x_0 \in X$, then $\langle x_0 \rangle \cap \bigcup_{x \in X \setminus \{x_0\}} \langle x \rangle = 0$.
If not, $nx_0 = n_1x_1 + \dots + n_rx_r$ for some nonzero $n_i \in \mathbb{N}$, $x_i \in X$
Thus, $F = \bigoplus_{x \in X} \langle x \rangle$

(ii) $\Rightarrow$ (iii) $\mathbb{Z}$ is the only infinite cyclic group.

(iii) $\Rightarrow$ (i) Suppose $F \cong \bigoplus_{i \in I} \mathbb{Z}$. Let $X = \{(0,\dots,0,1,0,\dots,0,\dots)\}$

By construction, this is a basis.

we have shown (i), (ii), (iii) are equivalent

(i, ii, iii) $\Rightarrow$ (iv) Let $X$ be a nonempty basis of $F$. Suppose $G$ is abelian gp with $f: X \to G$.

Define $\tilde{f} : F \to G$ by $\tilde{f}(\sum n_i x_i) = \sum n_i f(x_i)$

$$\begin{tikzcd}
 & G \\
X \arrow[ur, "f"] \arrow[r] & F \arrow[u, "\tilde{f}"']
\end{tikzcd}$$

(iv) => (i, ii, iii)

We will show $F \cong \bigoplus_{x \in X} \mathbb{Z}$

we showed above $\bigoplus_{x \in X} \mathbb{Z}$ is free in categorical sense

$$\begin{tikzcd}
 & F \\
X \arrow[ur] \arrow[r] \arrow[dr] & \bigoplus_{x \in X} \mathbb{Z} \arrow[u, dashed, "\psi"'] \\
 & F \arrow[u, dashed, "\varphi"']
\end{tikzcd}$$

Uniqueness $\Rightarrow \psi \circ \varphi = id$

So this is an isomorphism.

**Thm** A finitely generated abelian group is isomorphic to a direct sum of cyclic groups

**Lemma** If $G = \langle x_1, \dots, x_n \rangle$ is a f.g. abelian group, then $G/\langle x_1, \dots, x_{n-1} \rangle$ is cyclic.

**Pf** We claim $G/\langle x_1, \dots, x_{n-1} \rangle = \langle x_n + \langle x_1, \dots, x_{n-1} \rangle \rangle$

Let $y = a_1 x_1 + \dots + a_n x_n \in G$.

Then $y + \langle x_1, \dots, x_{n-1} \rangle = a_n x_n + \langle x_1, \dots, x_{n-1} \rangle = a_n (x_n + \langle x_1, \dots, x_{n-1} \rangle)$ ∎

**Pf of thm** Let $G = \langle x_1, \dots, x_n \rangle$. Let $C_i = G/\langle x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n \rangle$ be cyclic.

~~Then~~ Let $\pi_i : G \longrightarrow C_i$ be the quotient maps.

By Thm 8.2, there exists $\varphi : G \longrightarrow C_1 \oplus \dots \oplus C_n$ that factors through each $\pi_i$.

Each $\pi_i$ is surjective, so $i_i(C_i) \subset \operatorname{Im} \varphi$ for each $i$.

Thus $\varphi$ is surjective.

Suppose $y = a_1 x_1 + \dots + a_n x_n \in \operatorname{Ker} \varphi$ WLOG $a_i \nmid |x_i|$

Let $\sigma_i : C_1 \oplus \dots \oplus C_n \longrightarrow C_i$ be ith projection map

Then $\sigma_i \varphi(y) = \sigma_i(0) = 0$ for every $i$

But $\sigma_i \varphi(y) = \pi_i(y) = \pi_i(a_1 x_1 + \dots + a_n x_n) = a_i \pi_i(x_i)$

This is 0 only if $a_i \mid |x_i|$

$\Rightarrow$ each $a_i = 0$, so $y = 0$. Thus $\varphi$ is injective ∎

**Lemma 2.3** Let $m \in \mathbb{N}$, and write $m = p_1^{n_1} \cdots p_r^{n_r}$ for distinct primes $p_i$.

Then $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{n_r}}$

**Lemma** If $a, b \in \mathbb{N}$ are coprime, then $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \oplus \mathbb{Z}_b$

**Pf** Observe $\langle b \rangle = \{0, b, 2b, \ldots, (a-1)b\} \cong \mathbb{Z}_a$

$\langle a \rangle = \{0, a, 2a, \ldots, (b-1)a \cong \mathbb{Z}_b$

Note $\langle a \rangle \cap \langle b \rangle = 0$ (If $\lambda a = \mu b$ for some $\lambda < b, \mu < a$, then $b \mid \lambda$, $a \mid \mu$, so $\lambda = 0, \mu = 0$)

Then $\langle a \rangle \oplus \langle b \rangle$ is a subgroup of order $ab$, so it is all of $\mathbb{Z}_{ab}$. ⊙

**Pf of Lemma 2.3** Induct on $r$. If $r = 1$, trivial.

If $r > 1$, $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1} \cdots p_{r-1}^{n_{r-1}}} \oplus \mathbb{Z}_{p_r^{n_r}}$ by Lemma

$\cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_{r-1}^{n_{r-1}}} \oplus \mathbb{Z}_{p_r^{n_r}}$ by induction hypothesis ☒

**Thm 2.2** (Fundamental Theorem of Finitely Generated Abelian Groups)

Every finitely generated abelian group is isomorphic to a direct sum of cyclic groups, each of which is infinite or of prime power order.

**Pf** Thm + Lemma 2.3 ☒

**Def 4.1** Let $G$ be a group, and $S$ a set. An <u>action</u> is a map

$$G \times S \longrightarrow S \qquad \text{such that for all } x \in S,\ g_1, g_2 \in G$$
$$(g, x) \longmapsto g \cdot x \qquad 1)\ e \cdot x = x$$
$$2)\ (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$$

we say <u>$G$ acts on $S$</u>, sometimes write $G \circlearrowright S$

**Ex** $S_n$ acts on $\{1, \ldots, n\}$

**Ex** $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$

$$A \cdot \vec{v} = A\vec{v}$$

**Ex** $D_n$ acts on a regular $n$-gon

**Ex** $\mathbb{R}^n$ acts on itself by translation

$$v \cdot x = x + v$$

**Ex** Let $G$ be a group, $H$ a subgroup. Then $H$ acts on $G$ by (left) translation,

$$h \cdot g = hg$$

**Ex** Let $G$ be a group, $H$ a subgroup, $S = \{aH \mid a \in G\}$

$G$ acts on $S$ by translation

$$g \cdot aH = gaH$$

**Ex** Let $H \leq G$. $H$ acts on $G$ by conjugation

$$(h, g) \mapsto hgh^{-1}$$

**Thm 4.2** Let $G$ act on a set $S$

(i) The relation on $S$ given by $x \sim x' \iff gx = x'$ for some $g \in G$ is an equivalence relation

(ii) If $x \in S$, $G_x := \{g \in G \mid gx = x\}$ is a subgroup

**Def** The equivalence classes are called <u>orbits</u> (sometimes written $G\cdot x$)

$G_x$ is called the <u>stabilizer</u> of $x$.

An action is called <u>transitive</u> if there is exactly one orbit, i.e. for all $x, y \in S$ there exists $g \in G$ s.t. $g\cdot x = y$.

**Ex** Let $G$ act on itself by conjugation. An orbit of $x \in G$ $\{gxg^{-1} \mid g \in G\}$ is called a <u>conjugacy class</u> of $x$.

**Ex** Let $G$ act on its set of subgroups by conjugation. The stabilizer of a subgroup $K$ $N_G(K) = \{g \in G \mid gKg^{-1} = K\}$ is called the <u>normalizer</u> of $K$ in $G$.

Note that $K \trianglelefteq G \iff N_G(K) = G$.

**Thm 4.3** (orbit stabilizer theorem) Suppose $G$ acts on $S$. The size (cardinality) of the orbit of $x \in S$ equals the index of the stabilizer $[G:G_x]$

**Pf** Define a map

$$\{gG_x\} \longrightarrow G\cdot x$$
$$gG_x \longmapsto g\cdot x$$

well defined: Suppose $gG_x = hG_x \iff g^{-1}h \in G_x$
$$\iff g^{-1}h\cdot x = x$$
$$\iff h\cdot x = g\cdot x$$

Reverse argument shows map is injective, also surjective. ☒

**Cor 4.4** Let $G$ be a finite group, $K < G$.

(i) The number of elements in the conjugacy class of $x \in G$ is $[G : C_G(x)]$, where $C_G(x) = \{g \in G \mid gxg^{-1} = x\}$ is the <u>centralizer</u> of $x$.

(ii) If $x_1, \dots, x_n$ are representatives of the distinct conjugacy classes of $G$, then $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$

(iii) The number of subgroups of $G$ conjugate to $K$ is $[G : N_G(K)]$

**Def** The <u>class equation</u> is the equation $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$

**Thm 4.5** Let $G$ act on a set $X$. Then this induces a homomorphism $G \longrightarrow S(X)$.

**Pf** Let $g \in G$, Define $\mathcal{T}_g \in S(X)$ by $x \longmapsto g \cdot x$

Check that $\mathcal{T}_g$ is a bijection: $\mathcal{T}_{g^{-1}}$ is an inverse mapping for $\mathcal{T}_g$

the map $\varphi : G \longrightarrow S(X)$ $\quad \varphi(g) = \mathcal{T}_g$ is a homomorphism

$$\varphi(gh) = \mathcal{T}_{gh} \qquad \mathcal{T}_{gh}(x) = gh \cdot x$$

$$\varphi(g)\varphi(h) = \mathcal{T}_g \mathcal{T}_h \qquad \mathcal{T}_g(\mathcal{T}_h(x)) = \mathcal{T}_g(h \cdot x) = g \cdot (h \cdot x)$$

**Cor 4.6 (Cayley's Thm)** Let $G$ be a group. Then $G$ embeds in a symmetric group. (is isomorphic to a subgroup of)

**Pf** $G$ acts on itself by left translation, so we get a homomorphism

$$\varphi : G \longrightarrow S(G)$$

Compute $\operatorname{Ker} \varphi$: Suppose $\varphi(g) = id$
$$\varphi(g) = \mathcal{T}_g = id$$

Then $g \cdot x = x$ for all $x \in G$
$$g \cdot x = gx$$

i.e. $g = e$.

Thus $\operatorname{Ker} \varphi = \langle e \rangle$, so $\varphi$ is injective.

**Cor 4.7** Let $G$ be a group.

(i) For each $g \in G$, conjugation by $g$ induces an automorphism of $G$.
(these are called <u>inner automorphisms</u>)

(ii) There is a homomorphism $G \longrightarrow \operatorname{Aut} G$ whose kernel is the center of $G$ $\quad C(G) = \{g \in G \mid gx = xg$ for all $x \in G$.

**Pf** (i) $\tau_g : G \longrightarrow G$ is an automorphism
$x \longmapsto gxg^{-1}$

(ii) $\tau_g \tau_h = \tau_{gh}$, so the map $\begin{matrix} G \longrightarrow \mathrm{Aut}\,G \\ g \longmapsto \tau_g \end{matrix}$ is a homomorphism.

**Cor 4.10** Let $H < G$, and let $p$ be the smallest prime with $p \mid |G|$.
If $[G:H] = p$, then $H \lhd G$.

**Prop 4.8** Let $H < G$, and let $G$ act on the left cosets of $H$ by translation.
Then the kernel of the induced homomorphism $\varphi : G \longrightarrow S(\{gH\})$ is contained in $H$.

**Pf** Suppose $g \in \ker \varphi$, so $\varphi(g) = id$

$$\begin{aligned} &\varphi(g) = id \\ &\,\| \\ &\tau_g \end{aligned}$$

Then

$$\begin{aligned} &\tau_g(H) = H \\ &\,\| \\ &g \cdot H \\ &\,\| \\ &gH \qquad \Rightarrow \quad g \in H. \qquad \square \end{aligned}$$

**Cor 4.9** Let $H < G$ with $[G:H] = n$, and suppose $H$ contains no nontrivial normal subgroup of $G$. Then $G$ is isomorphic to a subgroup of $S_n$.

**Pf** Apply 4.8 to $H$: the map $G \longrightarrow S(\{gH\})$ must be injective.

Pf of 4.10 Let $X$ be the set of all left cosets of $H$ in $G$.

Let $K$ be the Kernel of map $G \longrightarrow S(X) \cong S_p$

$K \lhd G$, and by 4.8 $K \leq H$

Also, $G/K$ is isomorphic to a subgroup $S_p$

Thus, $|G/K| \mid p!$

But no prime smaller than $p$ divides $|G|$,

so we must have $|G/K| = p$ or $|G/K| = 1$

But $|G/K| = [G:K] = [G:H][H:K] = p[H:K]$

Thus $|G/K| = p$ and $[H:K] = 1$, i.e. $K = H$.

But $K$ was normal in $G$. $\blacksquare$