

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 \mathcal{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 \mathcal{C} , then $\bigcup_{i \in \mathbb{N}} S_i$ is linearly independent, hence ~~an upper bound~~ ^{an upper bound}.

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

Claim $V = \text{span } B$.

PF Suppose not: let $v \in V \setminus \text{span } B$.

Then $B \cup \{v\}$ is linearly independent $\Rightarrow B$ is not maximal \downarrow

□

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 $x' \in G$ s.t. $xx' = x'x = e$.

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 and 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' s.t. $x'x = e$.

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) $(1342) \in S_5$

Ex $(12)(13425) = (134)(25)$

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 $f: G \rightarrow H$ 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 $f: G \rightarrow G$, f is called an endomorphism
- An isomorphism $f: G \rightarrow G$ is called an automorphism.

Ex $\det: \text{GL}_n(\mathbb{K}) \rightarrow \mathbb{K}^*$ 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 $f: G \rightarrow H$ be a homomorphism.

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

Ex $\text{Ker } \det = \text{SL}_n(\mathbb{K})$

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

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

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

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

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

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

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

Cor 2.6 Any intersection of subgroups is a subgroup.

Def Let G be a group, and $X \subseteq G$ a subset.

then $\langle X \rangle = \bigcap_{\substack{H_i \leq G \\ X \subseteq H_i}} H_i$ is the subgroup generated by X

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 $\langle a^k \rangle = G \iff (k, m) = 1$

— x —

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

$$a \equiv b \pmod{m} \Leftrightarrow a-b \equiv 0 \pmod{m} \Leftrightarrow m \mid a-b \Leftrightarrow a-b \in \langle m \rangle$$

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 $a, b \in G$ $Ha = Hb \Leftrightarrow ab^{-1} \in H$
 $aH = bH \Leftrightarrow a^{-1}b \in H$

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

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

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

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

$$\begin{array}{ccc} \uparrow & & \uparrow \\ Ha_i & & Ha_t \end{array}$$

Since $b_j \in H$ Since $Kb_r \in H$

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

$$\text{then } b_j = Kb_r, \text{ so } Kb_j = Kb_r \Rightarrow b_j = b_r. \quad \square$$

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 ~~sub~~ 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 $|HK| = \frac{|H||K|}{|H \cap K|}$

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

$$\text{So } K = Ck_1 \sqcup Ck_2 \sqcup Ck_3 \sqcup \dots \sqcup Ck_n \text{ for some } k_i \in K$$

claim $HK = Hk_1 \sqcup Hk_2 \sqcup \dots \sqcup Hk_n$

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

Pf of claim Need to show

(1) HK_i and HK_j are disjoint

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

(3) $HK \supset HK_1 \sqcup \dots \sqcup HK_n$ (immediate)

(1) Suppose $h_i K_i \cap h_j K_j \neq \emptyset$. $h_i K_i = h_j K_j$

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

$$\Rightarrow K_j \in C K_i \Rightarrow K_j = K_i$$

(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, $H, K \leq G$, and suppose HK is a subgroup.

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



$$\text{w.w. } HK = KH \uparrow$$

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

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

well defined

Suppose $(H \cap K)h_1 = (H \cap K)h_2$, i.e. $h_1 h_2^{-1} \in H \cap K \leq K$, so $Kh_1 = Kh_2$

Surjective

clear

Injective

Suppose $\varphi((H \cap K)h_1) = \varphi((H \cap K)h_2)$

$$Kh_1 = Kh_2$$

$h_1 h_2^{-1} \in K$, 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, $H, K \leq G$ s.t. HK is a subgroup

If H, K are finite index in HK , then $[HK: H \cap K] = [HK: H][H: K]$

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 normal subgroup of G , denoted $N \triangleleft G$.

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 $D_8 = \langle r, s \mid r^4 = 1, s^2 = 1, srs = r^{-1} \rangle$

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

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

Remark: If $N \trianglelefteq G$ and $N \leq H \leq G$, then $N \trianglelefteq H$

Caution! $N \trianglelefteq K \trianglelefteq G$ does not imply $N \trianglelefteq G$!

Thm 5.3 Let G be a group, $K \leq G$, $N \trianglelefteq G$

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

(ii) $N \trianglelefteq \langle N, K \rangle$ (beware our notation $N \vee K$)

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

(iv) If $K \trianglelefteq G$ 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 $N \trianglelefteq G \Rightarrow axa^{-1} \in N$
 $x, a \in K \Rightarrow axa^{-1} \in K \Rightarrow axa^{-1} \in N \cap K$

(ii) Remark

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

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

Let $n_1 K_1 n_2 K_2 \dots n_r K_r \in \langle N, K \rangle$ ($n_i \in N, K_i \in K$)

Induction on n : If $r=1$, $n_1 K_1 \in NK$

If $r>1$: Assume $n_1 K_1 \dots n_{r-1} K_{r-1} = n_0 K_0 \in NK$

$$\begin{aligned} n_1 K_1 \dots n_{r-1} K_{r-1} n_r K_r &= n_0 K_0 n_r K_r \\ &= n_0 \underbrace{(K_0 n_r K_0^{-1})}_{\substack{\uparrow \\ N}} \underbrace{K_0 K_r}_{\substack{\uparrow \\ K}} \in NK \end{aligned}$$

(iv) $\underbrace{nK n^{-1} K^{-1}}_{\substack{\uparrow \\ K}} \in K \cap N = \langle e \rangle$, so $nK n^{-1} K^{-1} = e \Rightarrow nK = Kn$. \square

Thm 5.4 Let G be a group, $N \trianglelefteq G$. 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 $\tilde{a} = an_1$, $\tilde{b} = bn_2$
 Then $\tilde{a}\tilde{b} = an_1bn_2 = a(b(b^{-1}n_1b)n_2) \in abN$ \square

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

Ex \mathbb{Z} is abelian, so $\langle m \rangle \trianglelefteq \mathbb{Z}$. 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 $f: G \rightarrow H$ is a group hom., then $\text{Ker } f \trianglelefteq G$.
 (ii) If $N \trianglelefteq G$, then $\pi: G \rightarrow G/N$ is a (surjective) hom with $\text{Ker } \pi = N$
 $\pi(a) = aN$.

Pf (i) Let $x \in \text{Ker } f$, $a \in G$. Want $axa^{-1} \in \text{Ker } f$
 Compute $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)e f(a)^{-1} = e \Rightarrow axa^{-1} \in \text{Ker } f$

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

$$\pi(ab) = abN$$

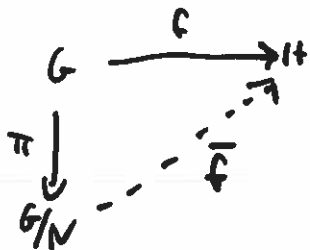
$$\pi(a)\pi(b) = aNbN = abN$$

So π is a homomorphism

$$\pi(a) = N \Leftrightarrow aN = N \Leftrightarrow a \in N \quad \square$$

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

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



pf Define $\bar{f}: G/N \rightarrow H$ 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 $n \in N$.

$$\bar{f}(aN) = f(a) = f(bn) = f(b)f(n) = f(b) = \bar{f}(bN) \quad \begin{array}{c} \uparrow \\ \text{since } N \subseteq \text{Ker } f \end{array}$$

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

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

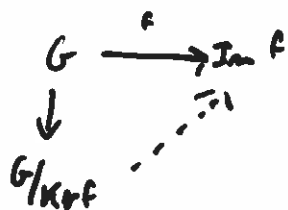
$$\bar{f}(aN) \bar{f}(bN) = f(a) f(b)$$

□

Remark $N \supseteq \text{Ker } f$, and $\text{Ker } \bar{f} = \text{Ker } f / N$

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

pf



Surjective by construction
Injective by remark

□

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

$$\text{Then } K/N \cap K \cong NK/N$$

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

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

claim $\ker \varphi = N \cap K$

If $a \in N \cap K$, $\varphi(a) = aN = N$ (since $a \in N$), so $a \in \ker \varphi$

If $a \in \ker \varphi$, $\varphi(a) = N$, so $a \in N \Rightarrow a \in N \cap K$.

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & NK/N \\ \downarrow & \nearrow \tilde{\varphi} & \\ K/N \cap K & & \end{array}$$

Since $N \cap K = \ker \varphi$, $\tilde{\varphi}$ is injective.

To see $\tilde{\varphi}$ surjective: Let $aN \in NK/N$

Since $NK = KN$, write $a = kn$ for some $k \in K, n \in N$.

Then $aN = knN = kN = \varphi(k)$.

$\Rightarrow \tilde{\varphi}$ is an isomorphism. □

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

Pf Let φ be the quotient map $G \rightarrow G/H$

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G/H \\ \downarrow & \nearrow \tilde{\varphi} & \\ G/K & & \end{array}$$

We get a surjective map $\tilde{\varphi}: G/K \rightarrow G/H$

Suppose $aK \in \ker \tilde{\varphi}$, so $\tilde{\varphi}(aK) = H$

"
alt, iff $a \in H$. Thus $H/K = \ker \tilde{\varphi}$

—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 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

suppose $\sigma_1 \dots \sigma_s = \tau_1 \dots \tau_r$ ~~not necessary~~

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:

$$\begin{aligned}(ab)(ab) &= id \\ (ab)(cd) &= (cd)(ab) \\ (ab)(ac) &= (bc)(ab) \\ (ab)(bc) &= (bc)(ac)\end{aligned}$$

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

Exercise It is the only subgroup of index 2 □

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 $\underline{S_n}$

i.e. If γ_1, γ_2 are 3-cycles $\gamma_1 = \sigma \gamma_2 \sigma^{-1}$ for some $\sigma \in S_n$

If σ is odd: choose 2 elements a, b not appearing in γ_2

Then $\tilde{\sigma} = \sigma(ab)$ is even, and $\tilde{\sigma} \gamma_2 \tilde{\sigma}^{-1} = \sigma(ab) \gamma_2 (ab) \sigma^{-1}$
 $= \sigma \gamma_1 \sigma^{-1}$
 $= \gamma_1$

□

Lemma Let $n \geq 5$. If $N \triangleleft A_n$ 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 3 $(ab)(ab) = \text{id}$. □

pf of Thm 6.10 Suppose $H \triangleleft A_n$ is nontrivial. We will show it contains a 3-cycle.
~~then~~ Cases: Disjoint cycle structure of elements of H

Case 1 Cycle of length $r \geq 4$

wlog $\sigma = (123 \dots r) \gamma$

Let $\delta = (123)$

$$\begin{aligned} H \ni \sigma^{-1} \delta \sigma \delta^{-1} &= \gamma^{-1} (r \dots 321) (123) (123 \dots r) \gamma (321) \\ &= (13r) \end{aligned}$$

Case 2 Multiple 3-cycles

wlog $\sigma = (123)(456) \gamma$

Let $\delta = (124)$

$$\begin{aligned} H \ni \sigma^{-1} \delta \sigma \delta^{-1} &= \gamma^{-1} (654)(321)(124)(123)(456) \gamma (421) \\ &= (14263) \end{aligned}$$

App'y Case 1

Case 3 Single 3-cycle

wlog $\sigma = (123)\gamma$

$$\exists \sigma^2 = (123)\gamma(123)\gamma = (123)^2\gamma^2 = (123)^2 = (123)^{-1} = (321)$$

Case 4

Product of transpositions

wlog $\sigma = (12)(34)\gamma$

Let $\delta = (123)$

$$\begin{aligned} \exists \sigma^{-1}\delta\sigma\delta^{-1} &= \gamma(34)(12)(123)(12)(34)\gamma(321) \\ &= (13)(24) \end{aligned}$$

Call this $\sigma_0 \in H$

Let $\delta_0 = (135)$

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

□

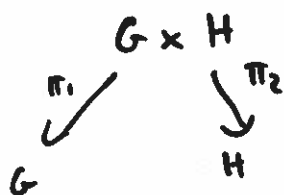
Def Let G, H be groups. The direct product $G \times H$ is the group
 $G \times H = \{ (g, h) \mid g \in G, h \in H \}$ (or direct sum)
 with operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

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

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

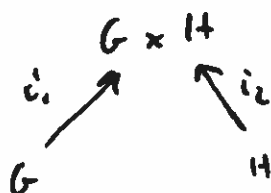
Fact $|G \times H| = |G| |H|$

Natural homomorphisms



$$\pi_1(g, h) = g$$

$$\pi_2(g, h) = h$$



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

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

Observe $\text{Ker } \pi_1 = i_1(G) \cong G$

$$G \times H / G \cong H$$

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

$$G \times H / H \cong G$$

Remark $G \times H$ is generated by $i_1(G), i_2(H)$

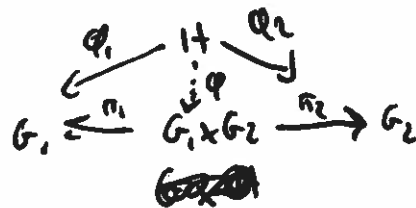
Def Let $\{G_i\}_{i \in I}$ be a collection of groups.

Then $\prod_{i \in I} G_i$ is a group called the direct product 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 $\varphi_1: H \rightarrow G_1$
 $\varphi_2: H \rightarrow G_2$.

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



PF $\varphi = (i_1 \varphi_1, i_2 \varphi_2)$

□

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 direct sum (or weak direct product) is the subgroup
of $\prod_{i \in I} G_i$ generated by the G_i .

It consists of elements with finitely many terms not equal to the identity.

Ex (A) $\prod_{i \in \mathbb{N}} \mathbb{Z}$

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

Ex Is $D_4 = \langle r, s \mid r^4 = 1, s^2 = 1, sr = r^{-1}s \rangle$ a direct product?

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

$$N = \langle r \rangle$$

$$H = \langle s \rangle$$

↑
Not normal!

Note that $D_4 = NH$ 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 for some $h \in H, n \in N$

(4) There exists a split exact sequence

$$1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1$$

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

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

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

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

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

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

(3) \Rightarrow (4)

$$1 \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$$

$\alpha =$ inclusion (injective)

$\sigma =$ inclusion

Define $\beta: G \rightarrow H$ by $\beta(hn) = h$.

Is β a homomorphism?

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

$$\beta(h_1 n_1) = h_1, \quad \beta(h_2 n_2) = h_2$$

$$\beta(h_1 n_1 h_2 n_2) = \beta(h_1 h_2 \underbrace{n_1 h_2}_{\substack{\uparrow \\ \text{in } N}} n_2) = h_1 h_2 = \beta(h_1 n_1) \beta(h_2 n_2)$$

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

(4) \Rightarrow (1) Suppose $1 \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$ 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 $h = \sigma\beta(x) \in \sigma(H)$

Claim $xh^{-1} \in \text{Ker } \beta = \alpha(N)$

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

$$\begin{aligned} \text{pf } \beta(xh^{-1}) &= \beta(x \sigma\beta(x)^{-1}) \\ &= \beta(x) \beta\sigma\beta(x)^{-1} \\ &= \beta(x) \beta(x)^{-1} \\ &= e \end{aligned}$$

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

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