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 non-empty 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 ~~an upper bound~~ 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 ⨍

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

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

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

<u>Notation 2</u> (cycle notation) $(1\ 3\ 4\ 2) \in S_5$

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

<u>Fact</u> Every element of S_n can be written as a product of disjoint cycles.

—— × ——

<u>Def</u> Let G, H be semigroups (resp. monoids, resp. groups). A <u>homomorphism</u>
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.

<u>Def</u> Let $f: G \to H$ be a homomorphism.
- The <u>kernel</u> of f is $\text{Ker } f = \{g \in G \mid f(g) = e\}$
- The <u>image</u> of f is $\text{Im } f = \{h \in H \mid h = f(g) \text{ for some } g \in G\}$

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

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

(i) f is injective $\Longleftrightarrow$ $\operatorname{Ker} f = \{e\}$

(ii) f is a bijective $\Longleftrightarrow$ thee exists a homomorphism $f': H \to G$
  s.t. $f f^{-1} = 1_H$ and $f'f = 1_G$

__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 $H \leq G$

__Fact__ If G a group, $H \subset G$ a subset, then H is a subgroup $\Longleftrightarrow$ 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
  $$\langle X \rangle = \bigcap_{\substack{H_i \leq G \\ X \subset H_i}} H_i \qquad \text{is the } \underline{\text{subgroup generated by } X}$$

__Thm 2.8__ $\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \mid a_i \in X, \; n_i \in \mathbb{Z} \right\}$

— 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, then a and a^{-1}
  are the only generators of G. If $|G| = m$, then $\langle a^k \rangle = G \Longleftrightarrow (k, m) = 1$

— x —

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 (rep. left) cosets $Ha = \{ha \mid h \in H\}$

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

Cor 4.3   (i & ii) The right (rep 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 $[G:G] = 1$ $[G : \langle e \rangle] = |G|$

(4)

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 $|I| = [G:H]$

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

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. $b_j a_i = Kb_r a_t$ for some $K \in K$.

$\underset{Ha_i}{\uparrow} \qquad \underset{Ha_t}{\uparrow}$

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

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

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

Cor [46] (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 $C = H \cap K$. $\quad C < K$, let $n = [K:C] = \dfrac{|K|}{|C|} = \dfrac{|K|}{|H \cap K|}$ (by Lagrange)

So $K = CK_1 \coprod CK_2 \coprod CK_3 \coprod \ldots \coprod CK_n$ for some $K_i \in K$

Claim $HK = HK_1 \coprod HK_2 \coprod \ldots \coprod HK_n$

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

(c)

<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 ~~both~~ ~~cosets~~ $h_i K_i = h_j K_j$

~~then~~ ~~~~ 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 $K = c K_i$ for some i, $c \in C$

Then $hk = (hc) K_i \in HK_i$ ▢

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

Then $[HK : K] = [H : H \cap K]$ and $[HK : H] = [\cancel{\text{~~~~~~~~}} K : H \cap K]$

HW: $HK = KH$

Pf We will construct bijection $\varphi : \{$right cosets of $H \cap K$ in $H\} \longrightarrow \{$right cosets of K 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. $h_1 h_2^{-1} \in H \cap K \leq K$, 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 $(H \cap K) h_1 = (H \cap K) h_2$ ▢

(7)

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

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 **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 $ab \in Na \Rightarrow aN \subseteq Na$.
Similarly, $Na \subseteq aN$. ∎

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 $N \triangleleft G$ and $N \subseteq H \leq G$, then $N \triangleleft H$ Caution! $N \triangleleft K \triangleleft G$ does not imply $N \triangleleft G$!

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

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

(ii) $N \triangleleft \langle N, K \rangle$ (bad ours notation $N \vee K$)

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

(iv) If $K \triangleleft G$ 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 $\begin{array}{l} N \triangleleft G \Rightarrow axa^{-1} \in N \\ x, a \in K \Rightarrow axa^{-1} \in K \end{array} \gg axa^{-1} \in N \cap K$.

(ii) Remark

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

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

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

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

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

      $n_1 K_1 \ldots n_{r-1} K_{r-1} n_r K_r = n_0 K_0 n_r K_r$

      $= n_0 \underbrace{(K_0 n_r K_0^{-1})}_{N} \underbrace{K_0 K_r}_{K} \in NK$.

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

Thm 5.4 Let G be a group, $N \triangleleft G$. 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 $\tilde{a} = a n_1$, $\tilde{b} = b n_2$

Then $\tilde{a}\tilde{b} = a n_1 b n_2 = a b (b^{-1} n_1 b) n_2 \in abN$ ∎

Def G/N is called the _quotient group_ or _factor group_ of G by N.

Ex $\mathbb{Z}$ is abelian, so $\langle m \rangle \triangleleft \mathbb{Z}$. 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 (1) If $f: G \longrightarrow H$ is a group hom., then $\ker f \triangleleft G$.
(2) If $N \triangleleft G$, then $\pi: G \longrightarrow G/N$ 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 $f(axa^{-1}) = f(a) f(x) f(a^{-1}) = f(a) e f(a)^{-1} = e$ $\Rightarrow axa^{-1} \in \ker f$

(2) Let $a, b \in G$. Want $\pi(ab) = \pi(a)\pi(b)$
$\pi(ab) = abN$
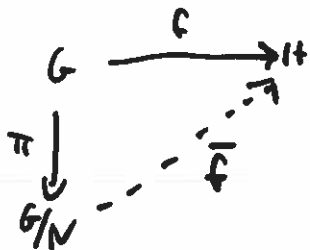$\pi(a)\pi(b) = aN bN = abN$ So π is a homomorphism

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

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

$$
\begin{array}{ccc}
G & \xrightarrow{\;f\;} & H \\
\pi \big\downarrow & \nearrow \raisebox{0.5ex}{$\scriptstyle \bar{f}$} & \\
G/N & &
\end{array}
$$

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

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

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

$\qquad\qquad\qquad\qquad\qquad\qquad \uparrow$ since $N \angle \ker f$

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

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

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

Remark $N \lhd \ker f$, and $\ker \bar{f} = \ker f / N$

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

Pf

$$
\begin{array}{ccc}
G & \xrightarrow{\;f\;} & \operatorname{Im} f \\
\big\downarrow & \nearrow \raisebox{0.5ex}{$\scriptstyle \bar{f}$} & \\
G/\ker f & &
\end{array}
$$
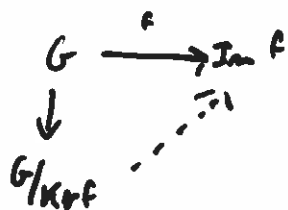
Surjective by construction
Injective by remark

$\blacksquare$

Corollary 5.9 (Second Isomorphism Theorem) Let G be a group, $K \leq G$, $N \triangleleft G$. 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 $\text{Ker } \varphi = N \cap K$

If $a \in N \cap K$, $\varphi(a) = aN = N$ (since $a \in N$), so $a \in \text{Ker } \varphi$

If $a \in \text{Ker } \varphi$, $\varphi(a) = N$, so $a \in N \Rightarrow a \in N \cap K$.

Since $N \cap K = \text{Ker } \varphi$, $\bar{\varphi}$ 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. $\blacksquare$

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

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

we get a surjective map $\bar{\varphi}: G/K \longrightarrow G/H$

Suppose $aK \in \text{Ker } \bar{\varphi}$, so $\bar{\varphi}(aK) = H$

$$\underset{aH}{\parallel} \quad , \quad \underset{\text{iff}}{\text{iff}} \quad a \in H. \quad \text{Thus } H/K = \text{Ker } \bar{\varphi}$$

— 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 $(x_1 x_2 \ldots x_r) = (x_1 x_r)(x_1 x_{r-1}) \ldots (x_1 x_3)(x_1 x_2)$

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 $(132) = \cancel{(13)(23)} (12)(13)$

(In general: odd length cycles are even)

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

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

      Spose $\sigma_1 \ldots \sigma_s = \tau_1 \ldots \tau_r$ ~~wlog~~

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

Pf of claim   Suppose $\tau_1 \ldots \tau_r = id$.   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   ∎

Def A_n is called the <u>alternating group</u>

Def A group G is called <u>simple</u> 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 $\sigma (x_1 \, x_2 \, \ldots \, x_r) \sigma^{-1} = (\sigma(x_1) \, \sigma(x_2) \, \ldots \, \sigma(x_r))$

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 τ_1, τ_2 are 3-cycles $\tau_1 = \sigma \tau_2 \sigma^{-1}$ 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 $\tilde{\sigma} \tau_2 \tilde{\sigma}^{-1} = \sigma (ab) \tau_2 (ab) \sigma^{-1}$
$$= \sigma \tau_2 \sigma^{-1}$$
$$= \tau_1 \qquad ∎$$

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 $(ab)(ab) = id.$ ☑

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

Case 1 Cycle of length $r \geq 4$

wLOG $\sigma = (123 \dots r)\,\gamma$

Let $\delta = (123)$

$H \ni \sigma^{-1}\delta\sigma\delta^{-1} = \gamma^{-1}(r \dots 321)(123)(123 \dots r)\gamma(321)$

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

Case 2 Multiple 3-cycles

wLOG $\sigma = (123)(456)\,\gamma$

Let $\delta = (124)$

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

$\qquad = (14263)$

Appl'y Case 1

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

   wLOG $\sigma = (123) \, \gamma$

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

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

   wLOG $\sigma = (12)(34) \, \gamma$

   Let $\delta = (123)$

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

   $\qquad \qquad \qquad = (13)(24)$

   Call this $\sigma_0 \in H$

   Let $\delta_0 = (135)$

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

   $\qquad \qquad \qquad = (135)$

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

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

(or <u>direct sum</u>)

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

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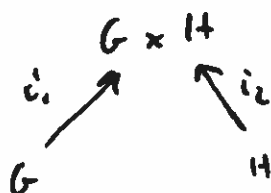
$$(1,1) + (0,2) = (1+0, 1+2) = (1,0)$$

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

<u>Natural homomorphisms</u>
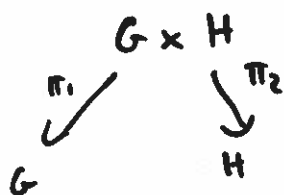
$\pi_1(g,h) = g$

$\pi_2(g,h) = h$

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

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

Observe $\quad \text{Ker } \pi_1 = i_2(G_2) \cong G_2$

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

$G \times H / G \cong H$

$G \times H / H \cong G$

Remark $\quad G \times H$ is generated by $i_1(G), i_2(H)$
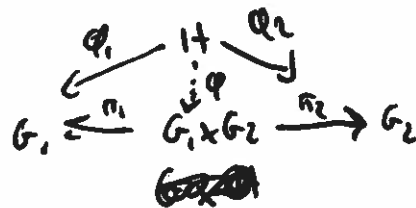
Def Let $\{ G_i \}_{i \in I}$ be a collection of groups.

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

(16)

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 $q_1 : H \to G_1$,
$$q_2 : H \to G_2.$$

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

PF $\varphi = (i_1 q_1, i_2 q_2)$

∅

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 <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 (a) $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}$

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

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

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

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

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
$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$$

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 $n_1, n_2 \in N$, $h_1, h_2 \in H$

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

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

$n_1 = n_2 \qquad h_1 = h_2$

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

(3) $\Rightarrow$ (4) $\quad 1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$ $\quad\sigma$

$\alpha =$ inclusion (injective)

$\sigma =$ inclusion

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

(19)

Is β a homomorphism?

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

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

$\beta(h_1 n_1 h_2 n_2) = \beta\left(h_1 h_2 \underline{h_2^{-1} n_1 h_2} \; n_2\right) = h_1 h_2 = \beta(h_1 n_1)\beta(h_2 n_2)$

$\uparrow N$

Note β surjective, and $\beta \circ \sigma = id$. Also $\ker \beta = Im \, \alpha$

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

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

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

Claim $x h^{-1} \in \ker \beta = \alpha(N)$

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

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

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

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

$\qquad\qquad = e$

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 $x = \sigma(e) = e$ ☑

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

<u>Def</u> Let X be a set.

Let X' be a set disjoint from X with $|X| = |X'|$

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

A <u>word</u> on X is a sequence $(a_1, a_2, a_3, \ldots)$

with $a_i \in X \cup X' \cup \{1\}$ that is eventually identically 1.

The <u>empty word</u> is $(1, 1, 1, \ldots)$

A word is <u>reduced</u> if a_i never equals a_{i+1}^{-1}

<u>Ex</u> $X = \{x, y\}$

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

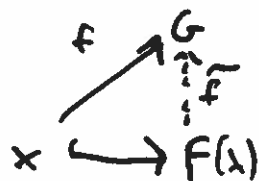$(x, y, x, y, y, 1, 1, 1, \ldots)$ is a reduced word   (Think: $xyxyy$)

Usually nonempty reduced words are written of form $x_1^{n_1} \ldots x_r^{n_r}$ $n_i \in \mathbb{Z} \setminus \{0\}, \; x_i \in X$

<u>Def</u> The set of all reduced words forms a group called the <u>free group on X</u> denoted $F(\lambda)$

<u>Thm 9.2</u> 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 $\tilde{f} : F_X \to G$
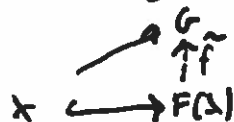

<u>pf</u> Define $\tilde{f}(x_1^{n_1} \ldots x_r^{n_r}) = f(x_1)^{n_1} \ldots f(x_r)^{n_r}$

<u>Cor 9.3</u> Every group is the homomorphic image of a free group.

<u>pf</u> Let X be a set of generators of G.   (Note: $G \cong {}^{F(\lambda)}/_{\ker \tilde{f}}$)

(21)

Thm-Def 1.1 Let F be an abelian group. TFAE

(i) F has a nonempty <u>basis</u>, i.e. a generating set X s.t. whenever $n_1 x_1 + \dots + n_k x_k = 0$ for s.e $n_i \in \mathbb{Z}$, $x_i \in X$, then $n_i = 0$ for all i.

(Thm 4: 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 $\tilde{F}: F \to G$

$$X \hookrightarrow F \quad \xrightarrow{\quad} G$$
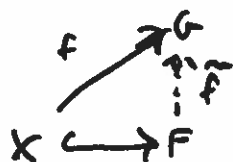
Pf (i) $\Rightarrow$ (ii) If $x \in X$, then $\langle x \rangle$ is infinite (cyclic) group

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, $n x_0 = n_1 x_1 + \dots + n_k x_k$ for some $n_i \in \mathbb{Z}$, $x_i \in X$

Thus, $F = \bigoplus_{x \in X} \langle x \rangle$

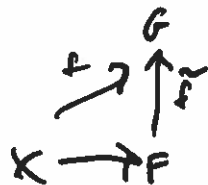(ii) $\Rightarrow$ (iii) $\mathbb{Z}$ is the only infinite cyclic group.

(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

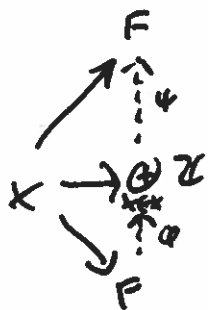(i, ii, iii) $\Rightarrow$ (iv) Let X be a nonempty basis of F. Suppose G is abelian gp with $f: X \to G$.

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

$$
\begin{array}{c}
G \\
\nearrow_f \uparrow \tilde{f} \\
K \longrightarrow F
\end{array}
$$

$(iv) \Rightarrow (i, ii, iii)$

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

$$
\begin{array}{c}
F \\
\nearrow \quad \uparrow \vdots \psi \\
K \longrightarrow \bigoplus_{x \in X} \mathbb{Z} \\
\searrow \quad \downarrow \vdots \varphi \\
F
\end{array}
$$

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

So this is an isomorphism.

(22)

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

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

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

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

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

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

Let $\pi_i : G \to C_i$ be the quotient maps.

By Thm 8.2, there exists $\varphi : G \to C_1 \oplus \ldots \oplus C_n$ that factors through each π_i.

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

Thus φ is surjective.

Suppose $y = a_1 x_1 + \ldots + a_n x_n \in \operatorname{Ker} \varphi$ wlog $a_i \times |x_i|$

Let $\sigma_i : C_1 \oplus \ldots \oplus C_n \to C_i$ be ith projection map

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

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

↑ This is 0 only if $a_i \mid |x_i|$

$\Rightarrow$ each $a_i = 0$, so $y = 0$. Thus φ 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 $b | \lambda$, $a | \mu$,

so $\lambda = \mu, \mu = 0$)

Then $\langle a \rangle \oplus \langle b \rangle$ is a subgroup of order ab, with is all of $\mathbb{Z}_{ab}$. $\quad\square$

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 $\square$

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 $\square$