

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 \bullet it has \bullet left \bullet inverses
exist and a left \bullet 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. $f f^{-1} = 1_H$ 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 $Kb_r \in H$

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

then $b_j = Kb_r$, so $Kb_j = Kb_r \Rightarrow b_j = b_r$. \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)

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

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

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

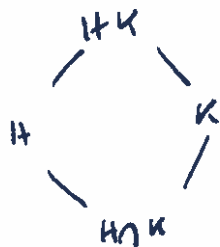
Then $K = cK_i$ for some $i, c \in C$

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



we: $HK = KH$

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) $\underbrace{nK n^{-1}}_{\substack{\uparrow \\ K}} k^{-1} \in K \cap N = \langle e \rangle$, so $nK n^{-1} k^{-1} = e \Leftrightarrow nK = Kn$. \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 $\pi(ab) = \pi(a)\pi(b)$

$$\pi(ab) = abN$$

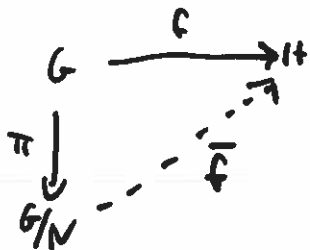
$$\pi(a)\pi(b) = aNbN = abN$$

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 $aN, bN \in G/N$.

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

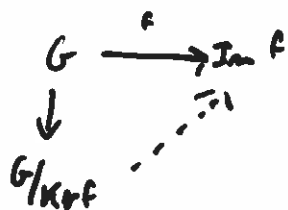
$$\bar{f}(aN) \bar{f}(bN) = f(a) f(b)$$

□

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 $(G/K)/(H/K) \cong G/H$

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

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

(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 $\delta_0 = (135)$

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

□

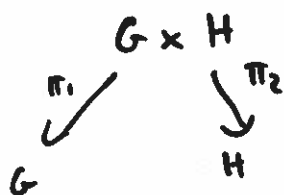
Def Let G, H be groups. The direct product $G \times H$ is the group
 $G \times H = \{ (g, h) \mid g \in G, h \in H \}$ (or direct sum)
 with operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

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

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

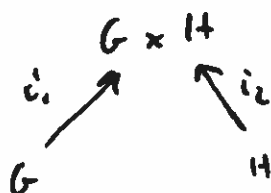
Fact $|G \times H| = |G| |H|$

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 $i_1(G), i_2(H)$

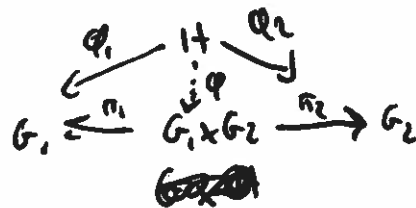
Def Let $\{G_i\}_{i \in I}$ be a collection of groups.

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) \mathbb{Z}

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

Ex Is $D_4 = \langle r, s \mid r^4 = 1, s^2 = 1, sr = sr^{-1} \rangle$ 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 $h_1 n_1, h_2 n_2 \in G$ $(h_1, h_2 \in H, n_1, n_2 \in N)$

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

$$\beta(h_1 n_1 h_2 n_2) = \beta(h_1 h_2 \underbrace{n_1 h_2 n_2}_{\substack{\uparrow \\ \beta^{-1}(h_2)}}) = h_1 h_2 = \beta(h_1 n_1) \beta(h_2 n_2)$$

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 $H \cong G/N$

Def Let X be a set.

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

choose a bijection $X \rightarrow X^{-1}$, 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: $xyxx^{-1}yy$)

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

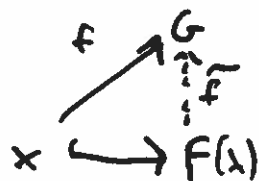
Usually nonempty reduced words are written of form $x_1^{n_1} \dots x_r^{n_r}$ $n_i \in \mathbb{Z} \setminus \{0\}$, $x_i \in X$

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 $f: X \rightarrow G$ is a map of sets ~~to~~ to a group G ,

there is a unique homomorphism $\tilde{f}: F(X) \rightarrow G$

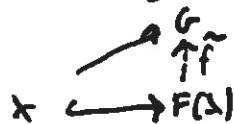


pf Define $\tilde{f}(x_1^{n_1} \dots x_r^{n_r}) = f(x_1)^{n_1} \dots f(x_r)^{n_r}$

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

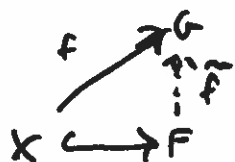
pf Let X be a set of generators of G .

(Note: $G \cong F(X)/\text{Ker } \tilde{f}$)



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

- (i) F has a nonempty basis, i.e. a generating set X s.t.
 whenever $n_1x_1 + \dots + n_kx_k = 0$ for s.t. $n_i \in \mathbb{Z}, x_i \in X$, 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 $f: X \rightarrow G$, there exists unique $\tilde{f}: F \rightarrow G$



PF (i) \Rightarrow (ii) If $x \in X$, the $\langle x \rangle$ 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, $n_0x_0 = n_1x_1 + \dots + n_kx_k$ 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.

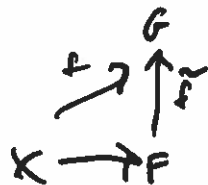
(iii) \Rightarrow (i) Suppose $F \cong \bigoplus_{i \in I} \mathbb{Z}$. Let $X = \{(0, \dots, 0, 1, 0, \dots, 0, \dots)\}$

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 group
 with $f: X \rightarrow G$.

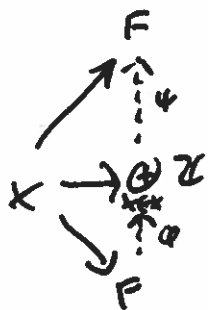
Define $\tilde{f}: F \rightarrow G$ by $\tilde{f}(\sum n_i x_i) = \sum n_i f(x_i)$



(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



Uniqueness $\Rightarrow \eta \circ \theta = \text{id}$

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

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.

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

By thm 8.2, there exists $\phi : G \rightarrow C_1 \oplus \dots \oplus C_n$ that factors through each π_i .

Each π_i is surjective, so $\phi_i(C_i) \subset \text{Im } \phi$ for each i .

Thus ϕ is surjective.

Suppose $y = a_1 x_1 + \dots + a_n x_n \in \text{Ker } \phi$ where $a_i \neq 0$

Let $\sigma_i : C_1 \oplus \dots \oplus C_n \rightarrow C_i$ be the projection maps

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

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

\uparrow
This is 0 only if $a_i \equiv 0$

\Rightarrow each $a_i = 0$, so $y = 0$. Thus ϕ is injective \square

Lemma 2.3 Let $m \in \mathbb{N}$, and write $m = p_1^{n_1} \dots p_r^{n_r}$ for distinct primes p_i .
Then $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{n_r}}$

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

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

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

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

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

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

$\cong \mathbb{Z}_{p_1^{n_1}} \oplus \dots \oplus \mathbb{Z}_{p_{r-1}^{n_{r-1}}} \oplus \mathbb{Z}_{p_r^{n_r}}$ 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

Def 4.1 Let G be a group, and S a set. An action is a map

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

we say G acts on S , sometimes write $G \curvearrowright S$

Ex S_n acts on $\{1, \dots, n\}$

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 $x \sim x' \iff \exists g \in G, gx = x'$ 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 orbits (sometimes with $G \cdot x$)

G_x is called the stabilizer of x .

An action is called transitive 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 conjugacy class 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 normalizer 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~~ Define a map

$$\begin{aligned} \{gG_x\} &\longrightarrow G \cdot x \\ gG_x &\longmapsto g \cdot x \end{aligned}$$

well-defined: Suppose $gG_x = hG_x$, $\iff \exists g'h \in G_x$

$$\iff g'h \cdot x = x$$

$$\iff g \cdot x = h \cdot x$$

Reverse argument shows ϕ is injective, also surjective. \square

Cor 4.4 Let G be a finite group, $K \trianglelefteq G$.

(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 centralizer 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 class equation 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 $G \rightarrow S(X)$.

PF Let $g \in G$, Define $\gamma_g \in S(X)$ by $x \mapsto g \cdot x$

Check that γ_g is a bijection: $\gamma_{g^{-1}}$ is an inverse mapping for γ_g

The map $\varphi: G \rightarrow S(X)$ $\varphi(g) = \gamma_g$ is a homomorphism

$$\varphi(gh) = \gamma_{gh}$$

$$\gamma_{gh}(x) = gh \cdot x$$

$$\varphi(g)\varphi(h) = \gamma_g \gamma_h$$

$$\gamma_g(\gamma_h(x)) = \gamma_g(h \cdot x) = g \cdot (h \cdot x)$$

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

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

Compute $\text{Ker } \varphi$: Suppose $\varphi(g) = \text{id}$
" γ_g

The ~~g~~ $g \cdot x = x$ for all $x \in G$
" gx

$$\text{i.e. } g = e.$$

This $\text{Ker } \varphi = \langle e \rangle$, so φ 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 inner automorphisms)

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

Pf (i) $\gamma_g : G \rightarrow G$ is an automorphism
 $x \mapsto gxg^{-1}$

(ii) $\gamma_g \gamma_h = \gamma_{gh}$, so the map $G \rightarrow \text{Aut } G$
 $g \mapsto \gamma_g$ 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 $H \trianglelefteq G$.

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 $\varphi: G \rightarrow S(\{gH\})$ is contained in H .

Pf Suppose $g \in \ker \varphi$, so $\varphi(g) = \text{id}$
 γ_g
 Then $\gamma_g(H) = H$
 $gH = H$
 $gH = H \Rightarrow g \in H. \quad \square$

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 the map $G \rightarrow S(\{gH\})$ 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 $G \rightarrow S(X) \cong S_p$

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

Also, G/K is isomorphic to a subgroup of 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 .

□

Motivation: ~~Cauchy's~~ ^{Lagrange's} theorem says if $H \leq G$, then $|H| \mid |G|$

when is converse true? If $m \mid |G|$, when must G have a subgroup of order m ?

Thm 5.2 (Cauchy's Theorem) If p is prime and $p \mid |G|$, then G has a subgroup of order p .



Lemma 5.1

Suppose H is a group of order p^n that acts on a set S .

Let $S_0 = \{x \in S \mid h \cdot x = x \text{ for all } h \in H\}$ = fixed points of action.

Then $|S| \equiv |S_0| \pmod{p}$

Pf

$$S = S_0 \sqcup H \cdot x_1 \sqcup H \cdot x_2 \sqcup \dots \sqcup H \cdot x_r$$

Orbit stabilizer: $|H x_i| = [H : H_{x_i}]$

\uparrow
must divide $|H| = p^n$

thus $p \mid |H x_i|$ for all i .



Pf of 5.2

Let $S = \{(a_1, \dots, a_p) \mid a_i \in G, a_1 a_2 \dots a_p = e\}$

Claim $\langle (123 \dots p) \rangle \leq S_p$ acts on S
 \uparrow
 \mathbb{Z}_p

If $(a_1, \dots, a_p) \in S$, is $(a_2, \dots, a_p, a_1) \in S$?

If $a_1 a_2 \dots a_p = e$, then $a_2 \dots a_p a_1 = a_1^{-1} (a_1 a_2 \dots a_p) a_1 = a_1^{-1} e a_1 = e$

$$a_2 \dots a_p a_1 = a_1^{-1} (a_1 a_2 \dots a_p) a_1 = a_1^{-1} e a_1 = e$$

Now $S_0 = \{(a, \dots, a) \mid a \in G, a^p = e\}$ (fixed points)

S_0 nonempty, $(e, \dots, e) \in S_0$, &

$$|S_0| \equiv |S| \pmod{p} \equiv |G|^{p-1} \pmod{p} \equiv 0 \pmod{p} \text{ since } p \mid |G|.$$

S_0 non-empty $\Rightarrow |S_0| > 0$, so there exists $a \in G \setminus \{e\}$ with $a^p = e$

Def A group is called a p-group if every element has order p^n for a fixed prime p and some $n \in \mathbb{N}$.

If G is a group, $H \leq G$ and H is a p -group, H is called a p-subgroup of G .

Ex \mathbb{Z}_{16} is a p -group.

Ex \mathbb{Z}_7 is a p -subgroup of \mathbb{Z}_{24}

Cor 5.3 A finite group G is a p -group $\Leftrightarrow |G| = p^n$ for some n .

PF \Leftarrow Lagrange's Theorem

\Rightarrow Suppose $q \mid |G|$ for some prime q . Then Cauchy's theorem ~~implies~~
implies G has an element of order $q \Rightarrow q = p$. \square

Cor 5.4 Every nontrivial finite p -group has a non-trivial center.

PF Suppose $|G| = p^n$ for some $n > 0$

class equation: $|G| = |Z(G)| + \sum [G : C_G(x_i)]$

\uparrow
multiple $|G| = p^n$

Thus $p \mid |Z(G)|$

\square

Lemma 5.5 Let G be finite, $H \leq G$ a p -subgroup. Then $[N_G(H) : H] \geq [G : H]$ and p .

PF Let S be set of left cosets of H
 H acts on S by left translation
what are fixed points?

$$\begin{aligned}
xH \in S_0 &\iff h x H = x H \quad \text{for all } h \in H \\
&\iff x^{-1} h x \in H \quad \text{for all } h \in H \\
&\iff x^{-1} H x = H \\
&\iff x \in N_G(H)
\end{aligned}$$

Thus $S_0 = \{xH \mid x \in N_G(H)\}$, so $|S_0| = [N_G(H):H]$

By Lemma 5.1, $|S_0| \equiv |S| \pmod{p}$, and $|S| \geq [G:H]$ □

Cor 5.6 Let G be finite, $H \leq G$ a ~~non-trivial~~ p -subgroup, and suppose $p \mid [G:H]$. Then $N_G(H) \neq H$

Pf By lemma, $[N_G(H):H] \equiv [G:H] \pmod{p} \equiv 0 \pmod{p}$.

Index always positive, so $[N_G(H):H] \geq p$ □

Thm 5.7 (First Sylow Theorem) Let G be a group of order $p^n m$ for a prime p , $p \nmid m$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$. Moreover, every subgroup of order p^i is normal in some subgroup of order p^{i+1} . (i < n)

Pf ~~transformation by conjugation~~

~~Induction~~

Claim If $H \leq G$ is a subgroup of order p^i ($1 \leq i \leq n$), then there is a subgroup H_1 of order p^{i+1} with $H \triangleleft H_1$.

Cauchy's Thm \Rightarrow subgroup of order p , claim + induction \Rightarrow theorem.

Pf of Claim

Suppose $H \leq G$, and $|H| = p^i$ for $1 \leq i < n$

Since $i < n$, $p \mid [G:H]$, so by Cor 5.6 $N_G(H) \neq H$

~~note $\sqrt{|N_G(H)|}$~~ $H \triangleleft N_G(H)$, so consider $N_G(H)/H$.

$$|N_G(H)/H| = [N_G(H):H] \stackrel{\text{Lemma 5.5}}{=} [G:H] \equiv 0 \pmod{p}$$

So $p \mid |N_G(H)/H|$, so it must contain a subgroup of order p ,

call it H_1/H . (for some $H_1 \leq N_G(H)$).

$$H \triangleleft H_1, \text{ and } |H_1| = |H| [H_1:H] = p^i p = p^{i+1}.$$

Def Let G be a group. A Sylow p -subgroup or p -Sylow subgroup is a maximal p -subgroup of G . First Sylow theorem \Rightarrow If $|G| = p^n m$, $p \nmid m$, then G has a Sylow p -subgroup of order p^n .

Cor 5.8 Let G have order $p^n m$ p prime, $p \nmid m$. Let H be a p -subgroup of G .

- (1) H is a Sylow p -subgroup $\iff |H| = p^n$
- (2) Every conjugate of a Sylow p -subgroup is a Sylow p -subgroup.
- (3) If there is only one Sylow p -subgroup, it is a normal subgroup.

Thm 5.9 (Second Sylow Theorem)

Any two p -Sylow subgroups are conjugate.

PF Let $P, Q \leq G$ be p -Sylow subgroups

Let $S = \{xP \mid x \in G\}$, and let Q act on S by translation.

Lemma 5.1 $\Rightarrow |S_0| \equiv [G:P] \pmod{p}$.

Since $p \nmid [G:P]$, $|S_0| > 0$

Let $xP \in S_0$, i.e. $q \cdot xP = xP$ for all $q \in Q$

$$x^{-1}qxP = P \quad \text{for all } q \in Q$$

$$x^{-1}qx \in P \quad \text{for all } q \in Q$$

$$x^{-1}Qx \leq P.$$

But $|x^{-1}Qx| = |Q| = |P|$, so $x^{-1}Qx = P$. \square

~~Corollary~~

Thm 5.10 (Third Sylow Theorem)

Let G be a finite group, P_1, \dots, P_r the p -Sylow subgroups for a fixed prime p .

Then $r \equiv 1 \pmod{p}$, and $r \mid |G|$.

PF Since P_1, \dots, P_r are all the conjugates of P_1 , ~~and~~
orbit stabilizer $\Rightarrow r = [G:N_G(P_1)]$ which must divide $|G|$.

Now let $S = \{P_1, \dots, P_r\}$, let P_1 act on S by conjugation.

Note $P_1 \in S_0$.

Suppose $P_i \in S_0$; then $xP_i x^{-1} = P_i$ for all $x \in P_1$.

In other words, $P_i \leq N_G(P_1)$

Note that P_1, P_i are p -Sylow subgroups of $N_G(P_1)$

and $P_i \trianglelefteq N_G(P_1)$

$$\Rightarrow P_i = P_1.$$

$$S_0 = \{P_1\}, \quad \text{Lemma 5.1} \Rightarrow r = |S| = |S_0| \equiv 1 \pmod{p} \quad \square$$

Prop 6.1 Let $|G| = pq$, for primes $p > q$. Then either
 $G \cong \mathbb{Z}_{pq}$ or $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$ (in which case $p \equiv 1 \pmod{q}$)

pf By Cauchy, let a have order p , b have order q .

Set $N = \langle a \rangle$, $H = \langle b \rangle$

Note $N \trianglelefteq G$, and $NH = G$ (since $|NH| = |N||H| = pq = |G|$), and $N \cap H = \{e\}$.

Thus $G \cong N \rtimes H$. (But sometimes this is a direct product).

Suppose G has r q -sylow subgroups. Then $r \equiv 1 \pmod{q}$, and $r \mid p-1$,
 thus $r=1$ or $r=p$.

If $r=1$, H is normal, direct product $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

If $r=p$, non-abelian semidirect product, and ~~restricted~~
 $p=r \equiv 1 \pmod{q}$ □

Cor 6.2 If p is an odd prime, a group of order $2p$ is either cyclic
 or the dihedral group D_p .

Prop 6.3 The groups of order 8 are either abelian, D_4 , or Q_8 .

pf Suppose $|G|=8$ is nonabelian. If $|a|=2$ for all $a \in G$, G is abelian.

So let $a \in G$ have order 4. Set $N = \langle a \rangle \trianglelefteq G$.

Case 1 Every element of $G \setminus N$ has order 2.

Let $b \in G \setminus N$, so $H = \langle b \rangle$ has order 2.

Note $H \cap N = \{e\}$, and $|HN| = |H||N| = 4 \cdot 2 = 8 = |G|$, so $HN = G$.

Thus $G \cong N \rtimes H = \mathbb{Z}_4 \rtimes \mathbb{Z}_2 = D_8$

Case 2 There exists $b \in G \setminus N$ of order 4

Let $K = \langle b \rangle$. Note $K \trianglelefteq G$

Note $|N \cap K| = \frac{|N||K|}{|NK|} = \frac{4 \cdot 4}{8} = 2$.

$\Rightarrow a^2 = b^2$

Since $N \trianglelefteq G$, $bab^{-1} \in N = \{e, a, a^2, a^3\}$

(i) $bab^{-1} = e \Rightarrow a = e \quad \downarrow$

(ii) $bab^{-1} = a \Rightarrow ba = ab \Rightarrow G \text{ abelian}$

(iii) $bab^{-1} = a^2 \Rightarrow ba^2b^{-1} = e \Rightarrow a^2 = e \quad \downarrow$

(iv) Thus, $bab^{-1} = a^3$

□

Prop 6.4 The nonabelian groups of order 12 are A_4 , D_6 , and $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$

pf Let P be a 3-Sylow subgroup. $|P|=3$, so $[G:P]=4$

Prop 4.8 $\Rightarrow \quad \varphi: G \rightarrow S_4$ with $\ker \varphi \leq P$

Case 1 $\ker \varphi = \{e\}$, then $G \leq S_4$, index 2 $\Rightarrow G \cong A_4$

Case 2 $\ker \varphi = P$, so $P \trianglelefteq G$, i.e. P is unique 3-Sylow subgroup.

Let K be a 2-Sylow subgroup, so $|K|=4$

Note $K \cap P = \{e\}$, $G = PK$ (since $|PK| = \frac{|P||K|}{|K \cap P|} = \frac{3 \cdot 4}{1} = 12 = |G|$)

$\Rightarrow G \cong \mathbb{Z}_3 \rtimes P \rtimes K$

Case (a) $K \cong \mathbb{Z}_4$, $G \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_4$

Case (b) $K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $G \cong \mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2) \cong D_6$

□

Motivating solvability

Quadratic: $x^2 + bx + c = 0$
 $(x + \frac{b}{2})^2 + c - \frac{b^2}{4} = 0$
 $x = -\frac{b}{2} \pm \sqrt{\frac{b^2}{4} - c}$

Cubic:
(Early 1500s)
del Ferro
Tartaglia
Cardano

$$x^3 + ax^2 + bx + c = 0$$

Substitute $x = y - \frac{a}{3}$

Reduces to solve depressed cubic $y^3 + py + r = 0$

Viète's substitution Let $y = w - \frac{p}{3w}$

$$(w - \frac{p}{3w})^3 + p(w - \frac{p}{3w}) + r = 0$$

$$w^3 + 3w^2(-\frac{p}{3w}) + 3w(-\frac{p}{3w})^2 + (-\frac{p}{3w})^3 + pw - \frac{p^2}{3w} + r = 0$$

$$w^3 - pw + \frac{p^2}{3w} - \frac{p^3}{27w^3} + pw - \frac{p^2}{3w} + r = 0$$

$$w^3 - \frac{p^3}{27w^3} + r = 0$$

$$w^6 + rw^3 - \frac{p^3}{27} = 0$$

Quadratic in w^3 !

$$w^3 = \frac{-r \pm \sqrt{r^2 + \frac{4p^3}{27}}}{2}$$

Ex $(x-1)(x-2)(x+3) = x^3 - 7x + 6$

$$w^3 = \frac{-6 \pm \sqrt{36 + \frac{4(-7)^3}{27}}}{2} = \frac{-6 \pm \sqrt{-400}}{2} = \frac{-6 \pm \frac{20}{3}i}{2} = -3 \pm \frac{10i}{3}$$

Quartic Formula : $x^4 + ax^3 + bx^2 + cx + d = 0$

(Ferrari, 1540)

Substitute $x = y - \frac{a}{4}$

suffices to solve $y^4 + qy^2 + ry + s = 0$

Suppose we can factor : $(y^2 + Ky + l)(y^2 - Ky^2 + m) = 0$

$$(1) \quad q = l + m - K^2$$

$$(2) \quad r = Km - Kl = K(m - l)$$

$$(3) \quad s = lm$$

$$(1') \quad m + l = q + K^2$$

$$(2') \quad m - l = \frac{r}{K}$$

$$(1' + 2') \quad 2m = K^2 + q + \frac{r}{K}$$

$$(1' - 2') \quad 2l = K^2 + q - \frac{r}{K}$$

So it suffices to find K in terms of q, r, s

$$(3), \quad 4s = 4lm = (K^2 + q + \frac{r}{K})(K^2 + q - \frac{r}{K})$$

$$4s = K^4 + 2K^2q + q^2 - \frac{r^2}{K^2}$$

$$0 = K^6 + 2qK^4 + (q^2 - 4s)K^2 - r^2$$

Cubic in K^2 !

Remark Like this proof, Ferrari's proof relies on cubic case - but proof of cubic case was not published until 1545

Def V.1.1 If A, K are fields with $A \subset K$, K is called a field extension of A .

Ex \mathbb{R} is an extension of \mathbb{Q} , \mathbb{C} is an extension of \mathbb{R} (and \mathbb{Q}).

Def V.3.1 Let A be a field, $f \in A[x]$. The splitting field of f over A is the smallest extension in which f splits (i.e. factors into linear terms) completely. It is the smallest field containing all roots of f .

Ex The splitting field of $x^2 - 2$ over \mathbb{Q} is $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$

Ex The splitting field of $x^2 + 1$ over \mathbb{R} is \mathbb{C}

Ex The splitting field of $x^3 - 2$ over \mathbb{Q} is $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$

Def V.4.1, V.4.2 Let A be a field, $f \in A[x]$, and E its splitting field. f is called solvable by radicals if there is a chain of extensions $A = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_t$ with $E \subset K_t$ and K_{i+1}/K_i is a simple radical extension, i.e. $K_{i+1} = K_i(\alpha_{i+1})$ for some α_{i+1} satisfying $\alpha_{i+1}^{n_{i+1}} \in K_i$.

Idea: "Formula for roots" \iff "Solvable by radicals"

Thm V.2.2 Let A be a field, $f \in A[x]$, and E its splitting field. Let $\sigma \in \text{Aut}_A E$ and $\alpha \in E$ a root of f . Then $\sigma(\alpha)$ is also a root of f .

pf Write $f = \sum_{i=0}^n a_i x^i$ for some $a_i \in A$. Then
$$0 = \sum_{i=0}^n a_i \alpha^i$$
$$0 = \sigma(0) = \sigma\left(\sum_{i=0}^n a_i \alpha^i\right) = \sum_{i=0}^n a_i \sigma(\alpha)^i$$

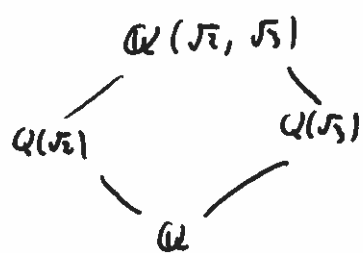
Def V.2.1 Let $A \subset K$ be an extension of fields. The Galois group of K over A is $\text{Gal}(K/A) := \text{Aut}_A K$

If $f \in A[x]$, the Galois group of f is the Galois group of its splitting field over A .

Thm (V.4.2) Let $f \in A[x]$ have n distinct roots. Then the Galois group of f is a subgroup of S_n .

Pf By Thm V.2.2, the Galois group acts on the set of distinct roots.

Ex Let $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$
splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.



Suppose $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$
 $\sigma(\sqrt{2}) = \pm\sqrt{2}$
 $\sigma(\sqrt{3}) = \pm\sqrt{3}$
 $\Rightarrow \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Thm (V.4.2) If $f \in A[x]$ is irreducible, its Galois group acts transitively on its roots.

Pf If α, β are two roots, $A(\alpha) \cong A(\beta)$ and this extends to an automorphism of the splitting field.

Thm A (V.2.5) Let p be prime, A a field containing a primitive p^{th} root of unity, and let $f = x^p - a \in A[x]$.

- (i) f is irreducible iff none of its roots are in A
- (ii) The splitting field of f is a simple radical extension
- (iii) If f is irreducible, its Galois group is \mathbb{Z}_p

pf (i) \Rightarrow Contrapositive: If a root lies in k , f has a linear factor so is reducible.

\Leftarrow Let α be a root. Then all of the roots are $\{\alpha, w\alpha, w^2\alpha, \dots, w^{p-1}\alpha\}$ for a primitive root of unity w .

Suppose $f = gh$ with $\deg g = m < p$.

Write $g = a_mx^m + \dots + a_0$. We may assume $a_m = 1$, so $a_0 = \pm \text{product of roots}$
 $= \pm w^r \alpha^m$
 for some $r \in \mathbb{M}$.

Since $a_0 \in k$, $w \in k$, we see $\alpha^m \in k$.

Note that $\gcd(m, p) = 1$, so $1 = ms + pt$ for some $s, t \in \mathbb{Z}$.

Then $\alpha = \alpha^{ms+pt} = (\alpha^m)^s (\alpha^p)^t \in k$.

(ii) The roots are $\{\alpha, w\alpha, \dots, w^{p-1}\alpha\}$. Since $w \in k$, the splitting field is $k(\alpha)$.

(iii) Let E be the splitting field of f , and let $\sigma \in \text{Gal}(E/k)$

Then $\sigma(\alpha) = w^i \alpha$ for some i , and this completely determines σ

Define $\text{Gal}(E/k) \longrightarrow \mathbb{Z}/p$

$(\alpha \mapsto w^i \alpha) \longmapsto i$

Immediate: homomorphism, injective

If f irreducible, $\text{Gal}(E/k)$ acts transitively \Rightarrow surjective. \square

Thm B (v.2.5) Let $k \subset K \subset E$ be fields where K, E are splitting fields of $f, g \in k[x]$

Then $\text{Gal}(E/k) \triangleleft \text{Gal}(E/K)$ and

$$\text{Gal}(E/k) / \text{Gal}(E/K) \cong \text{Gal}(K/k)$$

pf Define $\mathcal{B}: \text{Gal}(E/k) \longrightarrow \text{Gal}(K/k)$
 $\sigma \longmapsto \sigma|_K$

$\text{Ker } \mathcal{B} = \{\sigma \in \text{Gal}(E/k) \mid \sigma \text{ fixes } K\} = \text{Gal}(E/K)$

Since any element of $\text{Aut}_k K$ extends to $\text{Aut}_k E$, surjective. \square

Thm V.9.41 Let $f \in k[x]$ have degree n . Assume k contains p^{th} roots of unity for $p \leq n$.
 Let E be the splitting field of f over k . If f is solvable by radicals,
 then there exist subgroups $G_i \leq G := \text{Gal}(E/k)$ such that

- (i) $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_t = \langle e \rangle$
- (ii) $G_{i+1} \triangleleft G_i$
- (iii) G_i/G_{i+1} is cyclic of prime order for all i .

Pf Since f is solvable by radicals, there exist fields

$$k = k_0 \subset k_1 \subset \dots \subset k_t$$

with $E \subset k_t$ and k_{i+1}/k_i a simple radical extension.

i.e. $k_{i+1} = k_i(\beta_{i+1})$ for some β_{i+1} with $\beta_{i+1}^{r_{i+1}} \in k_i$

wlog each r_i is prime.

$$\text{Let } G_i = \text{Gal}(k_t/k_i)$$

Thm A \Rightarrow Each k_{i+1} is a splitting field

$$\text{Thm B} \Rightarrow G_{i+1} \triangleleft G_i$$

Thm B $\Rightarrow G_{i+1}/G_i \cong \text{Gal}(k_{i+1}/k_i)$ and Thm A $\Rightarrow \text{Gal}(k_{i+1}/k_i) \cong \mathbb{Z}/p$. \square

Def (cf. 7.9) Let G be a group. A subnormal series is a sequence

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_n = \langle e \rangle.$$

The quotients G_i/G_{i+1} are called factor groups

A finite group is called soluble if it has a normal series with each factor group cyclic of prime order.

In this language: A polynomial is soluble by radicals iff its Galois group is soluble.
we will see S_5 is not soluble

Ex Let $G = \mathbb{Z}_{30}$

* (1) $G \triangleright \langle 10 \rangle \triangleright 1$ is a (sub)normal series

$$G/\langle 10 \rangle \cong \mathbb{Z}_3 \quad \langle 10 \rangle/1 \cong \mathbb{Z}_2$$

* (2) $G \triangleright \langle 2 \rangle \triangleright \langle 6 \rangle \triangleright 1$

$$G/\langle 2 \rangle \cong \mathbb{Z}_3 \quad \langle 2 \rangle/\langle 6 \rangle \cong \mathbb{Z}_5 \quad \langle 6 \rangle/1 \cong \mathbb{Z}_2 \quad \text{is a soluble series}$$

Def 8.2 Let $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = 1$ be a subnormal series.

A refinement is a subnormal series $G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \dots \triangleright H_m = 1$

where G_0, \dots, G_n is a subsequence of H_0, \dots, H_m

Ex $G = \mathbb{Z}_{30}$

$G \triangleright \langle 5 \rangle \triangleright \langle 10 \rangle \triangleright 1$ is a refinement of *

$$G/\langle 5 \rangle \cong \mathbb{Z}_6 \quad \langle 5 \rangle/\langle 10 \rangle \cong \mathbb{Z}_2 \quad \langle 10 \rangle/1 \cong \mathbb{Z}_3$$

$G \triangleright \langle 2 \rangle \triangleright \langle 6 \rangle \triangleright 1$ is another refinement

$$G/\langle 2 \rangle \cong \mathbb{Z}_3 \quad \langle 2 \rangle/\langle 6 \rangle \cong \mathbb{Z}_5 \quad \langle 6 \rangle/1 \cong \mathbb{Z}_2$$

Def 8.3 A composition series is a subnormal series in which each factor group is simple

Ex \star $G \triangleright L_2 \triangleright L_6 \triangleright 1$ is a composition series
 $G/L_2 \cong \mathbb{Z}_2$ $L_2/L_6 \cong \mathbb{Z}_3$ $L_6/1 \cong \mathbb{Z}_5$

Remark A subnormal series is a composition series iff it does not admit a refinement.

Def 8.7 Two subnormal series are equivalent if there is a bijection between their sets of factor groups (up to isomorphism)

Thm 8.10 (Schröder Refinement Theorem) Let G be a group. Any two subnormal series of G admit equivalent refinements

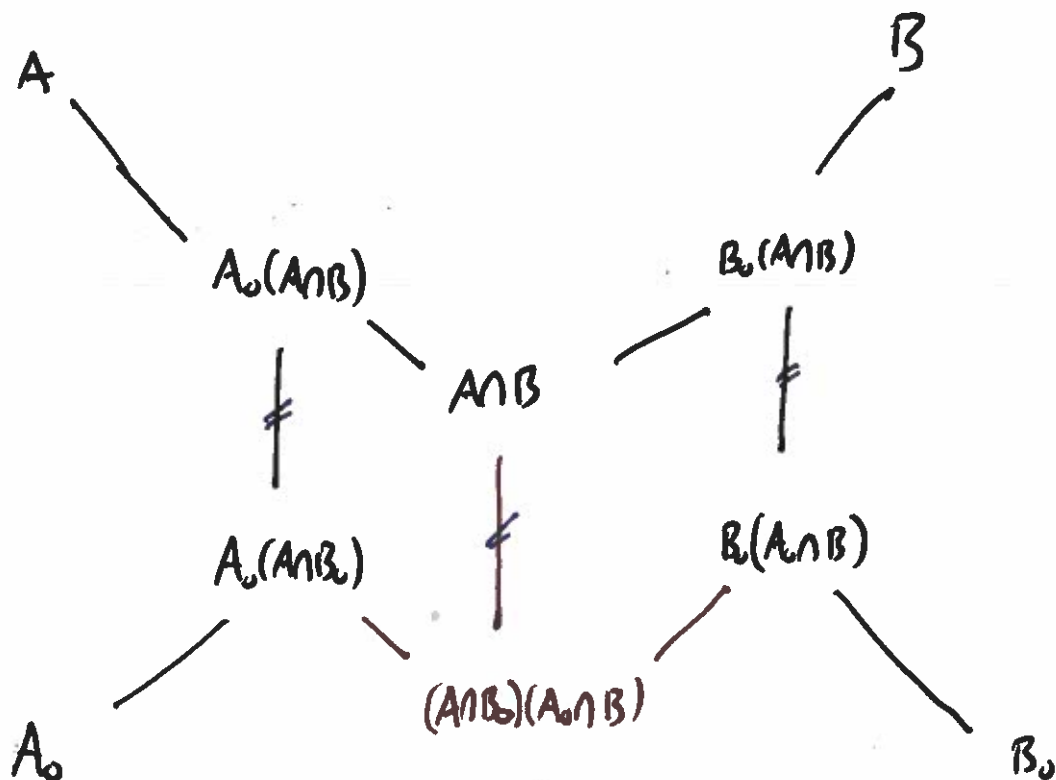
Ex \star and \star are not equivalent, but they admit equivalent refinements

Lemma 8.9 (Zassenhaus Lemma) Let G be a group, $A_0 \trianglelefteq A \leq G$ and $B_0 \trianglelefteq B \leq G$.

(i) $A_0(A \cap B_0) \trianglelefteq A_0(A \cap B)$

(ii) $B_0(A_0 \cap B) \trianglelefteq B_0(A \cap B)$

(iii) $A_0(A \cap B)/A_0(A \cap B_0) \cong B_0(A \cap B)/B_0(A_0 \cap B)$



Pf of 8.1 Note $A \cap B_0 = (A \cap B) \cap B_0 \triangleleft A \cap B$ (since $B_0 \triangleleft B$)
 and $A_0 \cap B = A_0 \cap (A \cap B) \triangleleft A \cap B$ (since $A_0 \triangleleft A$)

Thus $(A \cap B_0)(A_0 \cap B) \triangleleft A \cap B$

Claim $A_0(A \cap B) / A_0(A \cap B_0) \cong A \cap B / (A \cap B_0)(A_0 \cap B) \cong B_0(A \cap B) / B_0(A \cap B)$

Define $\varphi: A_0(A \cap B) \longrightarrow A \cap B / (A \cap B_0)(A_0 \cap B)$
 $a \longmapsto \bar{a}$

well defined: Suppose $a_1 c_1 = a_2 c_2$ for some $a_1, a_2 \in A_0$, $c_1, c_2 \in A \cap B$
 $c_1 c_2^{-1} = a_1^{-1} a_2 \in (A \cap B) \cap A_0 = A_0 \cap B \triangleleft (A \cap B_0)(A_0 \cap B)$
 $\Rightarrow \bar{c}_1 = \bar{c}_2$
 \uparrow since $c_1, c_2^{-1} \in A \cap B$ \uparrow since $a_1^{-1} a_2 \in A_0$

Surjective: \checkmark

Suppose $ac \in \ker \varphi$ for some $a \in A_0, c \in A \cap B$.

Then $c \in (A_0 \cap B)(A \cap B)$, so $c = c_1 c_2$ for some $c_1 \in A \cap B, c_2 \in A \cap B$.

Then $ac = (ac_1)c_2 \in A_0(A \cap B)$ so $\ker \varphi \subseteq A_0(A \cap B)$.

But $A_0(A \cap B) \subseteq \ker \varphi$, so $\ker \varphi = A_0(A \cap B)$. □

Pf of Thm 8.10

Let $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n$

$H = H_0 \triangleright H_1 \triangleright \dots \triangleright H_m$ be two subnormal series

Idea: Refine G by sticking H between G 's

Let $G_{n+1} = \langle e \rangle$

$H_{m+1} = \langle e \rangle$

Refine H by sticking G between H 's

smaller than G_0 , bigger than G_1 , normal seq. by Zassenhaus

$$G_0 = G_1(G_0 \cap H_0) \triangleright G_1(G_0 \cap H_1) \triangleright G_1(G_0 \cap H_2) \triangleright \dots \triangleright G_1(G_0 \cap H_m)$$

▽

$$G_1 = G_2(G_1 \cap H_0) \triangleright G_2(G_1 \cap H_1) \triangleright G_2(G_1 \cap H_2) \triangleright \dots \triangleright G_2(G_1 \cap H_m)$$

▽

$$G_2 = G_3(G_2 \cap H_0) \triangleright G_3(G_2 \cap H_1) \triangleright G_3(G_2 \cap H_2) \triangleright \dots \triangleright G_3(G_2 \cap H_m)$$

▽

⋮

▽

$$G_n = G_{n+1}(G_n \cap H_0) \triangleright G_{n+1}(G_n \cap H_1) \triangleright G_{n+1}(G_n \cap H_2) \triangleright \dots \triangleright G_{n+1}(G_n \cap H_m)$$

$$\begin{array}{ccccccc}
 H_0 & \triangleright & H_1 & \triangleright & \dots & \triangleright & H_m \\
 \text{"} & & \text{"} & & & & \text{"} \\
 H_1(H_0 \cap G_0) & & H_2(H_1 \cap G_0) & & & & H_{m+1}(H_m \cap G_0) \\
 \triangleright & & \triangleright & & & & \triangleright \\
 H_1(H_0 \cap G_1) & & H_2(H_1 \cap G_1) & & & & H_{m+1}(H_m \cap G_1) \\
 \triangleright & & \triangleright & & & & \triangleright \\
 \vdots & & \vdots & & & & \vdots \\
 \triangleright & & \triangleright & & & & \triangleright \\
 H_1(H_0 \cap G_n) & & H_2(H_1 \cap G_n) & & & & H_{m+1}(H_m \cap G_n)
 \end{array}$$

$$\text{Set } G(i, j) = G_{i+1}(G_i \cap H_j)$$

$$H(i, j) = H_{j+1}(H_j \cap G_i)$$

Need to show: (1) $G(i, j+1) \trianglelefteq G(i, j)$, $H(i+1, j) \trianglelefteq H(i, j)$
 For $0 \leq i < n$
 $0 \leq j < m$ (2) $G(i, j)/G(i, j+1) \cong H(i, j)/H(i+1, j)$] Zassenhaus!

$$(3) \quad G(i, m+1) = G(i+1, 0) \quad \text{and} \quad H(n+1, j) = H(0, j+1)$$

$$(3): \quad G(i, m+1) = G_{i+1}(G_i \cap H_{m+1}) = G_{i+1} = G(i+1, 0)$$

$$H(n+1, j) = H_{j+1}(H_j \cap G_{n+1}) = H_{j+1} = H(0, j+1)$$

□

Thm 8.11 (Jordan-Hölder Theorem) Any two composition series of a group are equivalent.

Cor 7.12 If $n \geq 5$, S_n is not solvable

PF $S_n \triangleright A_n \triangleright \langle e \rangle$ is a composition series with factor groups \mathbb{Z}_2, A_n . But A_n is not cyclic! □

Ex Let $f(x) = x^5 - x - 1$. Galois group is S_5 , so the roots of f cannot be expressed via radicals!

More general def Let G be a group. G is called solvable if it has a subnormal series with abelian factor groups

Remark Agrees with previous def for finite groups
 (Refine to a composition series, quotients are then simple & abelian, i.e. cyclic of prime order)

Thm 7.11 Let $H \trianglelefteq G$. G is soluble iff $H, G/H$ are both soluble.

PF \Rightarrow Let $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = 1$ be a soluble series for G .

(1) H is soluble: $H = G_0 \cap H \triangleright G_1 \cap H \triangleright \dots \triangleright G_n \cap H = 1$ is a subnormal series.

$$\begin{aligned} G_i \cap H / G_{i+1} \cap H &\cong G_{i+1} (G_i \cap H) / G_{i+1} \text{ by 2nd iso thm} \\ &\leq G_i / G_{i+1} \text{ which is abelian.} \end{aligned}$$

(2) Lemma If $\phi: G \rightarrow K$ a homomorphism, $\text{Im } \phi$ is soluble

PS wlog ϕ surjective

Then $K = \phi(G_0) \triangleright \phi(G_1) \triangleright \phi(G_2) \triangleright \dots \triangleright \phi(G_n) = 1$ is subnormal series

Natural maps $G_i \rightarrow \phi(G_i) \rightarrow \phi(G_i) / \phi(G_{i+1})$

Call this composition $\psi: G_i \rightarrow \phi(G_i) / \phi(G_{i+1})$

Note $G_{i+1} \leq \text{Ker } \psi$, so we see

$$\bar{\psi}: G_i / G_{i+1} \rightarrow \phi(G_i) / \phi(G_{i+1})$$

ψ surjective $\Rightarrow \bar{\psi}$ surjective

Then by 1st iso thm, $\phi(G_i) / \phi(G_{i+1})$ isomorphic to a quotient of G_i / G_{i+1} , so abelian.

\Leftarrow Let $G/H = \bar{K}_0 \supset \bar{K}_1 \supset \dots \supset \bar{K}_n = \bar{1}$ be solvable series for G/H .

Correspondence Theorem $\Rightarrow \bar{K}_i = K_i/H$ for some $K_i \supset K_{i-1}$

then $G = K_0 \supset K_1 \supset \dots \supset K_n = H$ and $K_i/K_{i+1} \cong K_i/H / K_{i+1}/H = \bar{K}_i/\bar{K}_{i+1}$

H solvable $\Rightarrow H$ has a solvable series

$H = K_{n+1} \supset K_{n+2} \supset \dots \supset K_m = 1$

then $G = K_0 \supset K_1 \supset \dots \supset K_n \supset K_{n+1} \supset \dots \supset K_m = 1$ is a solvable series. \square

Cor (i) $H \times K$ is solvable $\Leftrightarrow H, K$ solvable

(ii) $H \rtimes K$ is solvable $\Leftrightarrow H, K$ solvable.

Cor If G has order pq for distinct primes p, q , then G is solvable
Pf Prop 6.1 $\Rightarrow G \cong \mathbb{Z}_p$ or $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$ ($p > q$) \square

Cor Every finite p -group is solvable.

Pf Induct on $|G| = p^n$. $n=1 \Rightarrow G$ abelian, so solvable.

Class Equation $\Rightarrow G$ has a nontrivial center.

then $Z(G)$ is abelian, hence solvable, and $G/Z(G)$ is a smaller p -group and thus solvable by induction.

Exercise Every group of order p^2q for distinct primes p, q is solvable.

Thm If $161 < 60$, then G is Solvable

<u>pf</u>	1 ✓	16 p^4	31 p	46 p^2
	2 p	17 p	32 p^5	47 p
	3 p^2	18 p^2	33 p^4	48 *
	4 p^2	19 p^2	34 p^2	49 p^2
	5 p	20 p^2	35 p^4	50 p^2
	6 p^2	21 p^2	36 *	51 p^2
	7 p^3	22 p^2	37 p	52 p^2
	8 p^2	23 p	38 p^2	53 p
	9 p^2	24 *	39 p^2	54 *
	10 p^2	25 p^2	40 *	55 p^2
	11 p	26 p^2	41 p	56 *
	12 p^2	27 p^3	42 *	57 p^2
	13 p	28 p^2	43 p	58 p^2
	14 p^2	29 p	44 p^2	59 p
	15 p^2	30 *	45 p^2	

Idea: If all smaller groups are solvable, may assume G is simple.
(otherwise, there is a normal subgroup N with $N, G/N$ both solvable)

Case 1 $|G| = 24 = 2^3 \cdot 3$ wlog, G simple.

Suppose G has n_2 Sylow 2-subgroups.

$n_2 \equiv 1 \pmod{2}$, $n_2 | 24$, and G simple $\Rightarrow n_2 \neq 1$.

Thus $n_2 = 3$.

G acts on set of 2-Sylow subgroups $\Rightarrow \rho: G \rightarrow S_3$ must have nontrivial kernel.

Case 2 $|G| = 48 = 2^4 \cdot 3$ Same argument.

Case 3 $|G| = 30 = 2 \cdot 3 \cdot 5$ wlog G simple

$n_5 \equiv 1 \pmod{5}$, $n_5 | 6$

Simple $\Rightarrow n_5 = 6$

24 elements of order 5

$n_3 \equiv 1 \pmod{3}$, $n_3 | 10$

Simple $\Rightarrow n_3 = 10$

20 elements of order 3 \downarrow

Case 4 $|G| = 36 = 2^2 \cdot 3^2$ wlog G simple

$n_3 \equiv 1 \pmod{3}$, $n_3 | 4$

Simple $\Rightarrow n_3 = 4$

$\rho: G \rightarrow S_4$ must have nontrivial kernel

Case 5 $|G| = 40 = 2^3 \cdot 5$

$n_5 \equiv 1 \pmod{5}, n_5 | 8 \Rightarrow n_5 = 1$, not simple.

Case 6 $|G| = 42 = 2 \cdot 3 \cdot 7$

$n_7 \equiv 1 \pmod{7}, n_7 | 6 \Rightarrow n_7 = 1$, G not simple.

Case 7 $|G| = 54 = 2 \cdot 3^3$

$n_3 | 2, n_3 \equiv 1 \pmod{3} \Rightarrow n_3 = 1$, G not simple.

Case 8 $|G| = 56 = 2^3 \cdot 7$

$n_7 \equiv 1 \pmod{7}, n_7 | 8 \Rightarrow n_7 = 8$

48 elements of order 7
8 elements left $\Rightarrow n_2 = 1$, not simple. \square

~~408 elements of order 7, 8 elements left $\Rightarrow n_2 = 1$, not simple.~~

Thm (Burnside) If $|G| = p^a q^b$ then G is solvable.

Froit - Thompson Theorem If $|G|$ is odd, G is solvable.

(255 page paper!)

Alternative approach to solvability: Commutator subgroups

Def 7.7 Let G be a group. The commutator subgroup is

$$G^{(1)} = G' = [G, G] = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$$

Thm 7.8 $G' \trianglelefteq G$. Moreover, if $N \trianglelefteq G$, then G/N is abelian iff $G' \leq N$.

Pf Let $a \in G, xyx^{-1}y^{-1} \in G'$. $a(xyx^{-1}y^{-1})a^{-1} = (axa^{-1})(aya^{-1})(axa^{-1})^{-1}(aya^{-1})^{-1} \in G'$.
 \Leftarrow \checkmark If G/N is abelian, $abN = baN$ for all $a, b \in G$, so $aba^{-1}b^{-1} \in N \Rightarrow G' \leq N$ \square

Def $G^{(i)} = G^{(i+1)'} = [G^{(i)}, G^{(i-1)}]$ is the i^{th} derived subgroup.

Thy $G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \dots$ is a subnormal series if it terminates.

Thm G is solvable iff $G^{(n)} = \langle e \rangle$ for some n .

pf \Leftarrow By construction, $G^{(i)}/G^{(i+1)}$ is abelian.

\Rightarrow Suppose $G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n = \langle e \rangle$ is a solvable series.

then G_i/G_{i+1} is abelian.

Claim $G^{(i)} \leq G_i$

pf Induction on i . If $i=1$, G/G_1 abelian $\Rightarrow G' \leq G_1$

If $i > 1$, Assume $G^{(i-1)} \leq G_{i-1}$

then $G^{(i)} = G^{(i-1)'} \leq G_{i-1}'$

But G_{i-1}/G_i abelian $\Rightarrow G_{i-1}' \leq G_i$

Thy, $G^{(n)} \leq G_n = \langle e \rangle$

□

Def Let G be a group. The lower central series or descending central series

is $G = G_0 \supset G_1 \supset G_2 \supset \dots$

given by $G_i = [G, G_{i-1}]$

Remark Compare to the derived series $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$

Observe If $a \in G$, $x \in G_{i-1}$, then $[a, x] \in G_i$, so $G_{i-1}/G_i \leq Z(G/G_i)$

Def Let G be a group. A central series is a normal series

$1 = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_n = G$ with $H_0 \triangleleft G$

and $H_i/H_{i-1} \leq Z(G/H_{i-1})$

Ex After re-indexing, the lower central series is a central series if $G_n = 1$.

Def The upper central series or ascending central series is the series

$$1 = Z^0 \triangleleft Z^1 \triangleleft Z^2 \triangleleft \dots$$

defined by $Z^i/Z^{i-1} = Z(G/Z^{i-1})$

Thm Let G be a group with central series $1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$.
Then $G_j \leq H_{n-j} \leq Z^{n-j}$ for each $0 \leq j \leq n$.

PF (Claim) $H_i \leq Z^i$ for $0 \leq i \leq n$

Induct on i . $i=0$: $1 = H_0 = Z^0$

Suppose $i > 0$. ~~what to show~~
Let $x \in H_i$. Need to show $x \in Z^i$, i.e. $xZ^{i-1} \in Z(G/Z^{i-1})$

By assumption, $xH_{i-1} \in Z(G/H_{i-1})$

i.e. for any $y \in G$, $xyx^{-1}y^{-1}H_{i-1} = H_{i-1}$

i.e. $xyx^{-1}y^{-1} \in H_{i-1} \leq Z^{i-1}$ by inductive hypothesis

$$\text{So } xyx^{-1}y^{-1}Z^{i-1} = Z^{i-1}$$

$$\text{i.e. } xZ^{i-1} \in Z(G/Z^{i-1})$$

Claim 2 $G_j \leq H_{n-j}$ for $0 \leq j \leq n$

Induction j : $G_0 = G = H_n$

Let $x \in G_j$ be a commutator (generator)

$x = gyg^{-1}y^{-1}$ for some $g \in G$, $y \in G_{j-1} \leq H_{n-j+1}$

so $yH_{n-j} \in Z(G/H_{n-j})$

Then $xH_{n-j} = gyg^{-1}y^{-1}H_{n-j} = H_{n-j}$, so $x \in H_{n-j}$ \square

Def A group is called nilpotent if it has a finite central series.
 The smallest n such that $G_n = 1$ is called the class of G .
 G is nilpotent of class at most $n \iff G_n = 1 \iff Z^n = G$.

Thm 1) Every finite p -group is nilpotent.
 2) Nilpotent groups are solvable.

Pf 1) Finite p -groups have nontrivial centers + induction.
 2) $G^{(i)} \leq G_i$ □

Ex S_3 is solvable but not nilpotent.
 $Z'(S_3) = Z(S_3) = 1$, so not nilpotent.

Thm Let G be nilpotent of class c . Then every subgroup and quotient of G is nilpotent of class at most c .

Pf (i) Let $H \leq G$. Easy induction $\Rightarrow H_i \leq G_i$.

(ii) Let $N \trianglelefteq G$. We show by induction $(G/N)_i \leq G_i/N$.

$i=0$: $G/N = G_0/N$

$i>0$: $(G/N)_i = [G/N, (G/N)_{i-1}] \leq [G/N, G_{i-1}/N] = [G, G_{i-1}]/N = G_i/N$ □
↑
Induction

Ex Converse is not true: $S_3 \cong D_6$ not nilpotent.

Thm 7.1 If H, K are nilpotent, then $H \times K$ is nilpotent.

Pf Suffices to show $(H \times K)_i \leq H_i \times K_i$.

$i=0$: $(H \times K)_0 = H \times K = H_0 \times K_0$

$i>0$: $(H \times K)_i = [H \times K, (H \times K)_{i-1}] \leq [H \times K, H_{i-1} \times K_{i-1}] = [H, H_{i-1}] \times [K, K_{i-1}] = H_i \times K_i$ □
↑
Induction

Lemma 7.4 If G is nilpotent, it satisfies the normalizer condition,
i.e. every proper subgroup is properly contained in its normalizer.

Pf Let $H < G$. There exists n s.t. $G_{n+1} \leq H$ and $G_n \not\leq H$
then $[G_n, H] \leq [G_n, G] = G_{n+1} \leq H$, i.e. if $x \in G_n, h \in H$
then $xh x^{-1}h^{-1} \in H \Rightarrow xh x^{-1} \in H$
so $G_n \leq N_G(H)$
Then $H < HN_G(H) \leq N_G(H)$ \square

Prop 7.5 A finite group is nilpotent iff it is the direct product of its Sylow subgroups.

Pf \Leftarrow p -groups nilpotent, direct product of nilpotent groups is nilpotent.

\Rightarrow Let P be a p -Sylow subgroup

Claim $P \trianglelefteq G$

Pf Let $N = N_G(P)$, we will show $N_G(N) = N$.

Let $g \in N_G(N)$. Since $P \leq N$, $gPg^{-1} \leq N$.

$gPg^{-1} = P_2$ for some p -Sylow subgroup P_2 .

Also, $P_2 = hPh^{-1}$ for some $h \in N$.

i.e. $h^{-1}gPg^{-1}h = P$, so $h^{-1}g \in N$, i.e. $g \in N$.

$N_G(N) = N$ and G nilpotent $\Rightarrow N = G$, so $N_G(P) = G$, i.e. $P \trianglelefteq G$. \square

Let p_1, \dots, p_k be the primes dividing $|G|$

P_1, \dots, P_k corresponds the unique p_i -Sylow subgroups

then $P_i \cap P_1 \dots P_{i-1} P_{i+1} \dots P_k = \langle e \rangle$ for each i , and $G = P_1 \dots P_k$,

so $G \cong P_1 \times \dots \times P_k$ \square