# Preliminaries

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

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

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

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

**Ex Thm** Every vector space has a basis.

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

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

Zorn $\Rightarrow$ $C$ has a maximal element $B$.

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

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

$\boxtimes$

## Chapter 1

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

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

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

**Remark** Identity and inverses must be unique

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

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

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

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

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

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

**Remark** Also true for "right".

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

Symmetries of regular $n$-gon

**Ex** Symmetric group

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

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

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

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

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

—— x ——

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Cor 2.6** Any intersection of subgroups is a subgroup.

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

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

— x —

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

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

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

—— × ——

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

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

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

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

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

**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 $a, b \in G$ $\quad Ha = Hb \iff ab^{-1} \in H$

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

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

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

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

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

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

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

Suppose $Kb_ja_i = Kb_ra_t$, i.e. $b_ja_i = kb_ra_t$ for some $k \in K$.

$$\underbrace{b_ja_i}_{\in Ha_i} = \underbrace{kb_ra_t}_{\in Ha_t}$$

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 $Kb_j = Kb_r \Rightarrow b_j = b_r$. ∎

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

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

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

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

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

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

**Claim** $HK = HK_1 \amalg HK_2 \amalg \ldots \amalg HK_n$

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

Pf of claim Need to show

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

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

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

(1) Suppose $h_i K_i = h_j K_j$

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

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

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

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

Then $hK = (hc)K_i \in HK_i$ $\blacksquare$

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

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

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

HW: $HK = KH$

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

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

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

Surjective: clear

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

$Kh_1 = Kh_2$

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

**Prop 4.9** Let $G$ be a group, $H, K < G$ s.t. $HK$ is a subgroup

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

**Pf** Thm 4.5 + Prop 4.8 ∎

— x —

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

(i) Left cosets are right cosets

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

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

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

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

**Pf** (i) => (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) => (iii) Immediate.

(iii) => (iv) Immediate

(iv) => (i) Let $aN$ be a left coset.

If $b \in N$, $aba^{-1} \in N$, so $ab \in Na \Rightarrow aN \subset Na$.

Similarly, $Na \subset aN$. ∎

**Ex** In an abelian group, all subgroups are normal!

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

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

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

Remark: If $N \lhd G$ and $N < H < G$, then $N \lhd H$

Caution! $N \lhd K \lhd G$ does ~~not~~ imply $N \lhd G$!

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

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

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

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

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

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

(ii) Remark

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

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

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

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

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

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

(iv) $\overbrace{\underbrace{nKn^{-1}}_{\in K} K^{-1}}^{\in N} \in K \cap N = \langle e \rangle$, so $nKn^{-1}K^{-1} = e \Leftrightarrow nK = Kn$. $\blacksquare$

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

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

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

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

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

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

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

**Thm 5.5** (i) If $f: G \to H$ is a group hom., then $\text{Ker } f \lhd G$.

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

**Pf** (1) 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 $\pi$ is a homomorphism

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

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

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

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

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

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

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

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

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

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

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

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

$\blacksquare$

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

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

**Pf**

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

Surjective by construction
Injective by remark

$\blacksquare$

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

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

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

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

__Claim__ $\operatorname{Ker}\varphi = N \cap K$

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

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

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

Since $N \cap K = \operatorname{Ker}\varphi$, $\bar{\varphi}$ is injective.

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

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

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

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

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

__Pf__ Let $\varphi$ be the ~~composition~~ quotient map $G \longrightarrow G/H$

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

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

Suppose $aK \in \operatorname{Ker}\bar{\varphi}$, so $\bar{\varphi}(aK) = H$
$$\underset{aH}{\shortparallel}$$
, iff $a \in H$. Thus $H/K = \operatorname{Ker}\overline{\varphi}$

$\square$

—×—

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

* Can permute the cycles

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

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

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

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

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

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

(In general: odd length cycles are even)

**Thm 6.7** A permutation cannot be both even + odd.

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

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

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

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

Products of transpositions:
$$(ab)(ab) = id$$
$$(ab)(cd) = (cd)(ab)$$
$$(ab)(ac) = (bc)(ab)$$
$$(ab)(bc) = (bc)(ac)$$

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

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

**Pf** Define $\mathrm{Sgn}: S_n \longrightarrow \mathbb{Z}_2$ is a homomorphism with Kernel $A_n$.

**Exercise** It is the only subgroup of index 2 ∎

**Def** $A_n$ is called the **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** $\sigma\,(x_1\, x_2 \ldots x_r)\,\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \ldots\ \sigma(x_r))$

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

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

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

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

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

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

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

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

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

$= \tau_1$ ∎

**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 $(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d)$

Case 2 $(a\,b)(a\,c) = (a\,c\,b)$

Case 3 $(a\,b)(a\,b) = id.$ $\boxtimes$

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

Cases: Disjoint cycle structure of elements of $H$

Case 1 Cycle of length $r \geq 4$

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

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

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

Case 2 Multiple 3-cycles

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

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

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

Apply Case 1

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

wLOG $\sigma = (123)\tau$

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

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

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

Let $\delta = (123)$

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

$= (13)(24)$

Call this $\sigma_0 \in H$

Let $\delta_0 = (135)$

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

$= (135)$ $\blacksquare$

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

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

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

**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** $|G \times H| = |G|\,|H|$

<u>Natural homomorphisms</u>

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

$\pi_1(g,h) = g$

$\pi_2(g,h) = h$

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

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

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

**Observe** $\ker \pi_1 = i_1(G) \cong G$

$\ker \pi_2 = i_2(H) \cong H$

$G \times H / G \cong H$

$G \times H / H \cong G$

**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 <u>direct product</u> of $\{ G_i \}_{i \in I}$

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

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

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

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

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

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

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

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

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

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

**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 $N \cap H = \langle e \rangle$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad$ $HN$

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

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

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

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

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

(4) There exists a split exact sequence

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

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

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

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

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

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

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

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

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

$\sigma =$ inclusion

Is $\beta$ a homomorphism?

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

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

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

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

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

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

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

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

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

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

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

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

$= e$

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

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

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

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

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

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

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

A <u>word</u> on $X$ is a sequence $(a_1, a_2, a_3, \ldots)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ 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 $a_{i+1}^{-1}$

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

$(x, y, x, x, x^{-1}, y, y, 1, 1, 1, \ldots)$ 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 $x_1^{\lambda_1} \cdots x_r^{\lambda_r}$ $\lambda_r \in \mathbb{Z} \setminus \{0\}$, $x_i \in X$

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

**Thm 9.2** The free group is a free object in the category of groups.
In other words, if $f: X \longrightarrow G$ is a map of sets ~~to~~ to a group $G$, there is a unique homomorphism $\tilde{f}: F(X) \to G$

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

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

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

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

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

∎

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

(i) $F$ has a nonempty <u>basis</u>, i.e. a generating set $X$ s.t. whenever $n_1x_1 + \dots + n_k x_k = 0$ for some $n_i \in \mathbb{Z}$, $x_i \in X$, then $n_i = 0$ for all $i$.

(Think: no nontrivial linear combinations make zero $\Rightarrow$ no relations among generators)

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

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

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

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

<u>Pf</u> (i) $\Rightarrow$ (ii) If $x \in X$, then $\langle x \rangle$ is infinite (cyclic) group

Need to check: If $x_0 \in X$, then $\langle x_0 \rangle \cap \bigcup_{x \in X \setminus \{x_0\}} \langle x \rangle = 0$.

If not, $n x_0 = n_1 x_1 + \dots + n_r x_r$ for some nonzero $n_i \in \mathbb{N}$, $x_i \in X$

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

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

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

By construction, this is a basis.

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

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

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

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

---

(iv) $\Rightarrow$ (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

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

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

So this is an isomorphism.

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

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

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

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

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

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

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

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

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

Thus $\varphi$ is surjective.

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

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

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

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

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

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

▣

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

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

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

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

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

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

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

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

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

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

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

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

**Pf** Thm + Lemma 2.3 ☑

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

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

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

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

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

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

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

$$h \cdot g = hg$$

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

$G$ acts on $S$ by translation

$$g \cdot aH = gaH$$

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

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

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

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

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

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

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

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

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

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

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

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

**Pf** ~~Claim~~ Define a map

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

$$gG_x \longmapsto g\cdot x$$

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

$$\iff g^{-1}h\cdot x = x$$

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

Reverse argument shows map is injective, also surjective. ☒

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

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

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

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

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

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

**Pf** Let $g \in G$, Define $\tau_g \in S(X)$ by $x \longmapsto g \cdot x$

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

the map $\varphi : G \longrightarrow S(X)$ $\quad \varphi(g) = \tau_g$ is a homomorphism

$$\varphi(gh) = \tau_{gh} \qquad \tau_{gh}(x) = gh \cdot x$$

$$\varphi(g)\varphi(h) = \tau_g \tau_h \qquad \tau_g(\tau_h(x)) = \tau_g(h \cdot x) = g \cdot (h \cdot x)$$

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

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

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

Compute $\operatorname{Ker} \varphi$: Suppose $\underset{\tau_g}{\underset{\shortparallel}{\varphi(g)}} = id$

Then $\cancel{gx}\ \underset{gx}{\underset{\shortparallel}{g \cdot x}} = x$ for all $x \in G$

i.e. $g = e$.

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

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

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

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

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

(ii) $\gamma_g \gamma_h = \gamma_{gh}$, so the map $\begin{matrix} G \longrightarrow \operatorname{Aut} G \\ g \longmapsto \gamma_g \end{matrix}$ is a homomorphism.

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

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

**Pf** Suppose $g \in \operatorname{Ker} \varphi$, so

$$\begin{aligned} &\varphi(g) = id \\ &\quad \| \\ &\quad \gamma_g \end{aligned}$$

Then

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

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

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

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

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

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

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

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

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

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

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

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

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

Motivation: ~~Cauchy's~~ Lagrange's theorem says if $H < G$, 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 $|S| \equiv |S_0| \mod p$

**Pf** $S = S_0 \amalg H\cdot x_1 \amalg Hx_2 \amalg \cdots \amalg H\cdot x_r$

orbit stabilizer: $|Hx_i| = \underbrace{[H : H_{x_i}]}_{\text{must divide } |H| = p^n}$

thus $p \mid |Hx_i|$ for all $i$. ∎

**Pf of 5.2** Let $S = \{(a_1, \ldots, a_p) \mid a_i \in G, \ a_1 a_2 \cdots a_p = e\}$

Claim $\langle (1\,2\,3 \cdots p) \rangle < S_p$ acts on $S$
$\cong \mathbb{Z}_p$

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

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

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

$S_0$ nonempty, $(e, \ldots, e) \in S_0$,

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

$S_0$ nonempty $\Rightarrow |S_0| > 1$, so there exists $a \in G \setminus \{e\}$ with $a^p = e$ ∎

**Def** A group is called a <u>p-group</u> 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 <u>p-subgroup</u> of $G$.

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

**Ex** $\langle 3 \rangle$ is a p-subgroup of $\mathbb{Z}_{24}$

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

**Pf** $\Leftarrow$ LaGrange Theorem

$\Rightarrow$ S'pose $q \mid |G|$ for some prime $q$. Then Cauchy's Thm implies $G$ has an element of order $q \Rightarrow q = p$. $\blacksquare$

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

**Pf** S'pose $|G| = p^n$ for some $n > 0$

Class equation:
$$|G| = |Z(G)| + \sum \underbrace{[G : C_G(x_i)]}_{\text{must divide } |G| = p^n}$$

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

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

**Pf** Let $S$ be set of left cosets of $H$

$H$ acts on $S$ by left translation

what are fixed points?

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

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

By Lemma 5.1, $|S_0| \equiv |S| \bmod p$, and $|S| = [G:H]$ ∎

<u>Cor 5.6</u> Let $G$ be finite, $H \leq G$ a $p$-subgroup, and suppose $p \mid [G:H]$. Then $N_G(H) \neq H$

<u>Pf</u> By lemma, $[N_G(H):H] \equiv [G:H] \bmod p \equiv 0 \bmod p$.

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

<u>Thm 5.7 (First Sylow theorem)</u> 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 $(i < n)$ normal in some subgroup of order $p^{i+1}$.

<u>Pf</u>

<u>Claim</u> If $H < G$ is a subgroup of order $p^i$ $(1 \leq i < n)$, there is a subgroup $H_1$ of order $p^{i+1}$ with $H \lhd H_1$

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

**Pf of Claim** Suppose $H \le G$, and $|H| = p^i$ for $1 \le i < n$

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

$H \lhd N_G(H)$, so consider $N_G(H)/H$.

$$|N_G(H)/H| = [N_G(H):H] \equiv [G:H] \equiv 0 \mod p$$

Lemma 5.5

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

Call it $H_1/H$. (for some $H_1 \le N_G(H)$).

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

**Def** Let $G$ be a group. A <u>Sylow $p$-subgroup</u> or <u>$p$-Sylow subgroup</u> 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 $P, Q < G$ be p-Sylow subgroups

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

Lemma 5.1 $\Rightarrow$ $|S_0| \equiv [G:P] \bmod p$.

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

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

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

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

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

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

**Thm 5.10 (Third Sylow Theorem)**

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

Then $r \equiv 1 \bmod p$, and $r \mid |G|$.

**Pf** Since $P_1, \ldots, P_r$ are all the conjugates of $P_1$, which must divide $|G|$.

Orbit stabilizer $\Rightarrow$ $r = [G : N_G(P_1)]$

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

Note $P_1 \in S_0$.

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

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

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

and $P_i \lhd N_G(P_i)$

$\Rightarrow P_i = P_1$.

So $S_0 = \{P_1\}$, Lemma 5.1 $\Rightarrow$ $r = |S| \equiv |S_0| \equiv 1 \bmod p$ ☒

<u>Prop 6.1</u> 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 $p \equiv 1 \bmod q$)

<u>Pf</u> 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 $N \cap H = \langle e \rangle$.
Thus $G \cong N \rtimes H$. (But sometimes this is a direct product).

Suppose $G$ has $r$ $q$-sylow subgroups. Then $r \equiv 1 \bmod q$, and $r \mid pq$,
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
$p = r \equiv 1 \bmod q$ $\blacksquare$

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

<u>Prop 6.3</u> The groups of order 8 are either abelian, $D_4$, or $Q_8$.

<u>Pf</u> S'pose $|G| = 8$ is non abelian. If $|a| = 2$ for all $a \in G$, $G$ is abelian.
So let $a \in G$ have order 4. Set $N = \langle a \rangle \trianglelefteq G$.

<u>Case 1</u> Every element of $G \setminus N$ has order 2.
Let $b \in G \setminus N$, so $H = \langle b \rangle$ has order 2.
Note $H \cap N = \langle e \rangle$, and $|HN| = |H||N| = 4 \cdot 2 = 8 = |G|$, so $HN = G$.
Thus $G \cong N \rtimes H = \mathbb{Z}_4 \rtimes \mathbb{Z}_2 = D_8$

<u>Case 2</u> There exists $b \in G \setminus N$ of order 4
Let $K = \langle b \rangle$. Note $K \trianglelefteq G$
Note $|N \cap K| = \dfrac{|N||K|}{|NK|} = \dfrac{4 \cdot 4}{8} = 2$.
$\Rightarrow a^2 = b^2$

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

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

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

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

(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 $\Rightarrow$ $\varphi : G \longrightarrow S_4$ with $\operatorname{Ker}\varphi \leq P$

Case 1) $\operatorname{Ker}\varphi = \langle e \rangle$, then $G \leq S_4$, index 2 $\Rightarrow G \cong A_4$

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

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

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

$\Rightarrow G \cong$ ~~xxxx~~ $P \rtimes K$

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: $x^2+bx+c=0$

$$\left(x+\frac{b}{2}\right)^2+c-\frac{b^2}{4}=0$$

$$x=-\frac{b}{2}\pm\sqrt{\frac{b^2}{4}-c}$$

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

(Early 1500s)
del Ferro
Tartaglia
Cardano

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

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

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

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

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

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

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

$$w^6+rw^3-\frac{p^3}{27}=0 \qquad \text{Quadratic in } w^3!$$

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

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

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

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 : $(y^2 + Ky + \ell)(y^2 - Ky + m) = 0$

$$(1) \quad q = \ell + m - K^2$$
$$(2) \quad r = Km - K\ell = K(m-\ell)$$
$$(3) \quad s = \ell m$$

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

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

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

(3),
$$4s = 4\ell m = \left(K^2 + q + \frac{r}{K}\right)\left(K^2 + q - \frac{r}{K}\right)$$
$$4s = K^4 + 2K^2 q + q^2 - \frac{r^2}{K^2}$$
$$0 = K^6 + 2qK^4 + (q^2 - 4s)K^2 - r^2$$

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 $k, K$ are fields with $k \subset K$, $K$ is called a field extension of $k$.

**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 $k$ be a field, $f \in k[x]$. The splitting field of $f$ over $k$ 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.9.1, V.9.2** Let $k$ be a field, $f \in k[x]$, and $E$ its splitting field. $f$ is called solvable by radicals if there is a chain of extensions

$$k = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_t$$

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 $\alpha_{i+1}$ satisfying $\alpha_{i+1}^{n_{i+1}} \in K_i$.

Idea: "Formula for roots" $\Longleftrightarrow$ "Solvable by radicals"

**Thm V.2.2** Let $k$ be a field, $f \in k[x]$, and $E$ its splitting field. Let $\sigma \in \mathrm{Aut}_k E$ 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 $a_i \in k$. Then

$$0 = \sum_{i=0}^{n} a_i \alpha^i$$

$$0 = \sigma(0) = \sigma\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} a_i \sigma(\alpha)^i$$

$\blacksquare$

<u>Def V.2.1</u> Let $k \subset K$ be an extension of fields. The <u>Galois group</u> of $K$ over $k$ is $\quad \mathrm{Gal}(K/k) := \mathrm{Aut}_k K$

If $f \in k[x]$, the <u>Galois group of $f$</u> is the Galois group of its splitting field over $k$.

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

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

<u>Ex</u> Let $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$

splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

Suppose $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}\right)$

$\sigma(\sqrt{2}) = \pm\sqrt{2}$

$\sigma(\sqrt{3}) = \pm\sqrt{3}$

$\Rightarrow \mathrm{Gal}\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}\right) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

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

<u>Pf</u> If $\alpha, \beta$ are two roots, $k(\alpha) \cong k(\beta)$ and this extends to an automorphism of the splitting field.

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

(i) $f$ is irreducible iff none of its roots are in $k$

(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 $\alpha$ be a root. Then all of the roots are $\{\alpha, \omega\alpha, \omega^2\alpha, \ldots, \omega^{p-1}\alpha\}$ for a primitive root of unity $\omega$.

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

Write $g = a_m x^m + \cdots + a_0$. We may assume $a_m = 1$, so $a_0 = \pm$ product of roots $= \pm\, \omega^r \alpha^m$ for some $r \in \mathbb{N}$.

Since $a_0 \in k$, $\omega \in k$, 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 $\{\alpha, \omega\alpha, \ldots, \omega^{p}\alpha\}$. Since $\omega \in k$, the splitting field is $k(\alpha)$.

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

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

Define
$$\mathrm{Gal}(E/k) \longrightarrow \mathbb{Z}_p$$
$$(\alpha \mapsto \omega^i \alpha) \longmapsto i$$

Immediate: homomorphism, injective

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

**Thm B (V.25)** Let $k \subset K \subset E$ be fields where $K, E$ are splitting fields of $f, g \in k[x]$.

Then $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/k)$ and

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

Pf Define
$$\Phi: \mathrm{Gal}(E/k) \longrightarrow \mathrm{Gal}(K/k)$$
$$\sigma \longmapsto \sigma|_K$$

$\ker \Phi = \{\sigma \in \mathrm{Gal}(E/k) \mid \sigma \text{ fixes } K\} = \mathrm{Gal}(E/K)$

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

Thm V.9.4 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 $G_i \leq G := Gal(E/k)$ such that

(i) $G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \langle e \rangle$

(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

$$k = K_0 \subset K_1 \subset \cdots \subset K_t$$

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 $\beta_{i+1}$ with $\beta_{i+1}^{r_{i+1}} \in K_i$

WLOG each $r_i$ is prime.

Let $G_i = Gal(K_t/K_i)$

Thm A => Each $K_{i+1}$ is a splitting field

Thm B => $G_{i+1} \triangleleft G_i$

Thm B => $G_{i+1}/G_i \cong Gal(K_{i+1}/K)$ and Thm A => $Gal(K_{i+1}/K_i) \cong \mathbb{Z}_p$. ∎

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

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \langle e \rangle .$$

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

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

☆ (2) $G \trianglerighteq \langle 2 \rangle \trianglerighteq \langle 6 \rangle \trianglerighteq 1$

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

**Def 8.2** Let $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = 1$ be a subnormal series.
A refinement is a subnormal series $G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_m = 1$
where $G_0, \ldots, G_n$ is a subsequence of $H_0, \ldots, H_m$

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

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

$G/\langle 5 \rangle \cong \mathbb{Z}_5$ $\quad \langle 5 \rangle / \langle 10 \rangle \cong \mathbb{Z}_2$ $\quad \langle 10 \rangle / 1 \cong \mathbb{Z}_3$

$G \trianglerighteq \langle 2 \rangle \trianglerighteq \langle 10 \rangle \trianglerighteq 1$ is another refinement

$G/\langle 2 \rangle \cong \mathbb{Z}_2$ $\quad \langle 2 \rangle / \langle 10 \rangle \cong \mathbb{Z}_5$ $\quad \langle 10 \rangle / 1 \cong \mathbb{Z}_3$

**Def 8.3** A <u>composition series</u> is a subnormal series in which each factor group is simple

**Ex** ☆ $G \triangleright \langle 2 \rangle \triangleright \langle 6 \rangle \triangleright 1$ is a composition series

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

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

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

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

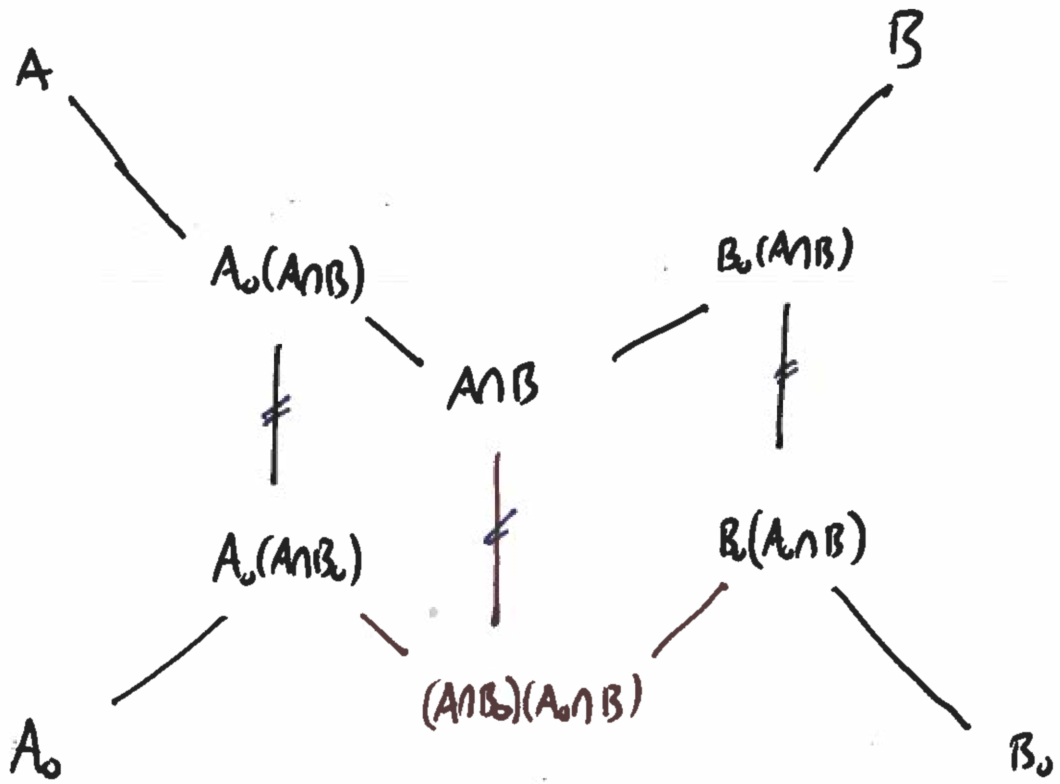
**Ex** * and ☆ are not equivalent, but they admit equivalent refinements

**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 8.9** Note $A\cap B_0 = (A\cap B)\cap B_0 \trianglelefteq A\cap B$ (since $B_0 \trianglelefteq B$)

and $A_0\cap B = A_0\cap (A\cap B) \trianglelefteq A\cap B$ (since $A_0 \trianglelefteq A$)

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

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

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

well defined: Suppose $a_1c_1 = a_2c_2$ for some $a_1, a_2 \in A_0$, $c_1, c_2 \in A\cap B$

$$c_1c_2^{-1} = a_1^{-1}a_2 \in \underset{\text{since } c_1c_2^{-1}\in A\cap B}{(A\cap B)} \cap \underset{\text{since } a_1^{-1}a_2\in A_0}{A_0} = A_0\cap B \leq (A\cap B_0)(A_0\cap B)$$

$\Rightarrow \bar{c}_1 = \bar{c}_2$

Surjective: ✓

Suppose $ac \in \operatorname{Ker} \varphi$ for some $a \in A_0$, $c \in A \cap B$.

Then $c \in (A_0 \cap B)(A \cap B_0)$, so $c = c_1 c_2$ for some $c_1 \in A_0 \cap B$, $c_2 \in A \cap B_0$)

Then $ac = (ac_1)c_2 \in A_0(A \cap B_0)$ so $\operatorname{Ker}\varphi \leq A_0(A \cap B_0)$

But $A_0(A \cap B_0) \leq \operatorname{Ker}\varphi$, so $\operatorname{Ker}\varphi = A_0(A \cap B_0)$ $\square$

<u>Pf of Thm 8.10</u> Let $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n$

$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m$ be two subnormal series

Idea: Refine $G_\cdot$ by sticking $H_\cdot$ between $G$'s

Refine $H_\cdot$ by sticking $G_\cdot$ between $H$'s

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

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

smaller than $G_0$, bigger than $G_1$, normal sg. by Zassenhaus

$$
\begin{array}{ccccccccc}
G_0 & = G_1(G_0 \cap H_0) & \trianglerighteq & G_1(G_0 \cap H_1) & \trianglerighteq & G_1(G_0 \cap H_2) & \trianglerighteq \cdots & \trianglerighteq & G_1(G_0 \cap H_m) \\
\triangledown & & & & & & & & \\
G_1 & = G_2(G_1 \cap H_0) & \trianglerighteq & G_2(G_1 \cap H_1) & \trianglerighteq & G_2(G_1 \cap H_2) & \trianglerighteq \cdots & \trianglerighteq & G_2(G_1 \cap H_m) \\
\triangledown & & & & & & & & \\
G_2 & = G_3(G_2 \cap H_0) & \trianglerighteq & G_3(G_2 \cap H_1) & \trianglerighteq & G_3(G_2 \cap H_2) & \trianglerighteq \cdots & \trianglerighteq & G_3(G_2 \cap H_m) \\
\triangledown & & & & & & & & \\
\vdots & & & & & & & & \\
\triangledown & & & & & & & & \\
G_n & = G_{n+1}(G_n \cap H_0) & \trianglerighteq & G_{n+1}(G_n \cap H_1) & \trianglerighteq & G_{n+1}(G_n \cap H_2) & \trianglerighteq \cdots & \trianglerighteq & G_{n+1}(G_n \cap H_m)
\end{array}
$$

$$
\begin{array}{ccccccc}
H_0 & \trianglerighteq & H_1 & \trianglerighteq & \cdots & \trianglerighteq & H_m \\
\shortparallel & & \shortparallel & & & & \shortparallel \\
H_1(H_0 \cap G_0) & & H_2(H_1 \cap G_0) & & & & H_{m+1}(H_m \cap G_0) \\
\triangledown & & \triangledown & & & & \triangledown \\
H_1(H_0 \cap G_1) & & H_2(H_1 \cap G_1) & & & & H_{m+1}(H_m \cap G_1) \\
\triangledown & & \triangledown & & & & \triangledown \\
\vdots & & \vdots & & & & \vdots \\
\triangledown & & \triangledown & & & & \triangledown \\
H_1(H_0 \cap G_n) & & H_2(H_1 \cap G_n) & & & & H_{m+1}(H_m \cap G_n)
\end{array}
$$

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: For $0 \le i \le n$, $0 \le j \le m$

(1) $G(i,j+1) \lhd G(i,j)$ , $H(i+1,j) \lhd H(i,j)$
(2) $G(i,j)/G(i,j+1) \cong H(i,j)/H(i+1,j)$ ] Zassenhaus!

(3) $G(i,m+1) = G(i+1,0)$ and $H(n+1,j) = H(0,j+1)$

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

∎

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 $S_n \rhd A_n \rhd \langle e \rangle$ 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 $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_n = 1$ be a soluble series for $G$.

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

$$G_i \cap H / G_{i+1} \cap H \cong G_{i+1}(G_i \cap H) / G_{i+1} \quad \text{by } 2^{\text{nd}} \text{ iso thm}$$

$$\leq G_i / G_{i+1} \quad \text{which is abelian.}$$

(2) **Lemma** If $\varphi : G \to K$ a homomorphism, $\operatorname{Im} \varphi$ is soluble

**Pf** WLOG $\varphi$ surjective

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

Natural maps $G_i \longrightarrow \varphi(G_i) \longrightarrow \varphi(G_i)/\varphi(G_{i+1})$

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

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

$$\bar{\psi} : G_i / G_{i+1} \longrightarrow \varphi(G_i)/\varphi(G_{i+1})$$

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

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

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

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

then $G = K_0 \trianglerighteq K_1 \trianglerighteq \cdots \trianglerighteq K_n = H$ and $K_i/K_{i+1} \cong {}^{K_i/H}\big/_{K_{i+1}/H} = {}^{\bar{K}_i}\big/_{\bar{K}_{i+1}}$

$H$ solvable $\Rightarrow$ $H$ has a solvable series

$H = K_{n+1} \trianglerighteq K_{n+2} \trianglerighteq \cdots \trianglerighteq K_m = 1$

Then $G = K_0 \trianglerighteq K_1 \trianglerighteq \cdots \trianglerighteq K_n \trianglerighteq K_{n+1} \trianglerighteq \cdots \trianglerighteq K_m = 1$ is a solvable series. ∎

<u>Cor</u> (i) $H \times K$ is solvable $\Leftrightarrow$ $H, K$ solvable

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

<u>Cor</u> If $G$ has order $pq$ for distinct primes $p, q$, then $G$ is solvable

<u>Pf</u> Prop 6.1 $\Rightarrow$ $G \cong \mathbb{Z}_{pq}$ or $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$ $(p > q)$ ∎

<u>Cor</u> Every finite $p$-group is solvable.

<u>Pf</u> 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.

<u>Exercise</u> Every group of order $p^2q$ for distinct primes $p, q$ is solvable.

**Thm** If $|G| < 60$, then $G$ is soluble

**pf**

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

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

**Case 1** $|G| = 24 = 2^3 \cdot 3$. WLOG, $G$ simple.
Suppose $G$ has $n_2$ Sylow 2-subgroups.
$n_2 \equiv 1 \bmod 2$, $n_2 \mid 24$, and $G$ simple $\Rightarrow n_2 \neq 1$.
Thus $n_2 = 3$.
$G$ acts on set of 2-Sylow subgroups $\Rightarrow$ $\rho : G \longrightarrow S_3$ 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

$n_5 \equiv 1 \bmod 5$, $n_5 \mid 6$ Simple $\Rightarrow n_5 = 6$ 24 elements of order 5

$n_3 \equiv 1 \bmod 3$, $n_3 \mid 10$ Simple $\Rightarrow n_3 = 10$ 20 elements of order 3 $\lightning$

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

$n_3 \equiv 1 \bmod 3$, $n_3 \mid 4$ Simple $\Rightarrow$ $n_3 = 4$

$\rho : G \longrightarrow S_4$ must have nontrivial Kernel

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

$n_5 \equiv 1 \bmod 5$, $n_5 \mid 8$ $\Rightarrow n_5 = 1$, not Simple.

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

$n_7 \equiv 1 \bmod 7$, $n_7 \mid 6$ $\Rightarrow n_7 = 1$, $G$ not Simple.

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

$n_3 \mid 2$, $n_3 \equiv 1 \bmod 3$ $\Rightarrow n_3 = 1$, $G$ not simple.

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

$n_7 \equiv 1 \bmod 7$, $n_7 \mid 8 \Rightarrow n_7 = 8$ 48 elements of order 7
8 elements left $\Rightarrow n_2 = 1$, not simple. $\square$

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

**Feit-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 $a \in G$, $xyx^{-1}y^{-1} \in G'$. $a(xyx^{-1}y^{-1})a^{-1} = (axa^{-1})(aya^{-1})(axa^{-1})^{-1}(aya^{-1})^{-1} \in G'$.

$\Leftarrow$ ✓

$\Rightarrow$ 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** $G^{(i)} = G^{(i-1)'} = [G^{(i-1)}, G^{(i-1)}]$ is the $i^{\text{th}}$ derived subgroup.

Thus $G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$ is a subnormal series if it terminates.

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

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

$\Rightarrow$ Suppose $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \langle e \rangle$ is a soluble 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 $\Rightarrow G_{i-1}' \leq G_i$

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

— x —

**Def** Let $G$ be a group. The <u>lower central series</u> or <u>descending central series</u>

is $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots$

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

$1 = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_n = G$ with $H_i \trianglelefteq G$

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 <u>upper central series</u> or <u>ascending central series</u> is the series

$$1 = Z^0 \lhd Z^1 \lhd Z^2 \lhd \cdots$$

defined by $\quad Z^i / Z^{i-1} = Z\left(G / Z^{i-1}\right)$

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

**Pf** <u>Claim 1</u> $H_i \le Z^i$ for $0 \le i \le n$

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

Suppose $i > 0$. ~~~~ 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 $y \in G$, $\quad xyx^{-1}y^{-1}H_{i-1} = H_{i-1}$

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

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

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

<u>Claim 2</u> $G_j \le H_{n-j}$ for $0 \le j \le n$

Induction on $j$: $\quad G_0 = G = H_n$

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

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

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 $x \in H_{n-j}$ ∎

**Def** A group is called <u>nilpotent</u> if it has a finite central series. The smallest $n$ such that $G_n = 1$ is called the <u>class</u> 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) $G^{(i)} \leq G_i$ $\square$

**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 $N \lhd G$. We show by induction $(G/N)_i \leq G_i/N$

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

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

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

**Thm 7.3** If $H, K$ are nilpotent, then $H \times K$ is nilpotent

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

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

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

**Lemma 7.4** If $G$ is nilpotent, it satisfies the <u>normalizer condition</u>, 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 $G_n \nleq H$

Then $[G_n, H] \leq [G_n, G] = G_{n+1} \leq H$, i.e. if $x \in G_n$, $h \in H$

then $xhx^{-1}h^{-1} \in H \Rightarrow xhx^{-1} \in H$

so $G_n \leq N_G(H)$

Then $H < HG_n \leq N_G(H)$ ☐

**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

<u>Claim</u> $P \trianglelefteq G$

<u>Pf</u> 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. $P \trianglelefteq G$. ☐

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

$P_1, \ldots, P_k$ ~~corresponding~~ the unique $p_i$ - Sylow subgroups

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

so $G \cong P_1 \times \cdots \times P_k$ ☐

**Def 1.1** A ring is a nonempty set $R$ with two binary operations $+$ and $\cdot$ satisfying

(1) $(R,+)$ is an abelian group

(2) $(R,\cdot)$ is a semigroup

(3) $a(b+c) = ab+ac$ for all $a,b,c \in \mathbb{R}$.
$(a+b)c = ac+bc$

If multiplication is commutative, $R$ is called a commutative ring

If $(R,\cdot)$ is a monoid, $R$ is called a unital ring or a ring with 1 or a ring with unity

Ex $\mathbb{Z}$ is a commutative ring with 1.
Ex $\mathbb{Z}_n$ is a commutative ring with 1.
Ex $M_n(\mathbb{R})$ is a non-commutative ring with 1.

**Thm 1.2** Let $R$ be a ring.

(i) $0\cdot a = a\cdot 0 = 0$ for all $a \in R$

(ii) $(-a)b = a(-b) = -(ab)$ for all $a,b \in \mathbb{R}$

(iii) $(-a)(-b) = ab$ for all $a,b \in R$

(iv) $(na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$, $a,b \in R$.

(v) $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$ for all $a_i, b_j \in R$

Pf (i) $0\cdot a = (0+0)\cdot a = 0a + 0a$, so $0 = 0a$

(ii) $ab + (-a)\cdot b = (a+(-a))b = 0\cdot b = 0$, so $(-a)b = -(ab)$

(iii) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$

(iv) $(na)\cdot b = (a+\dots+a)b = ab+\dots+ab = n(ab)$

(v) Distributive property $\blacksquare$

**Def 1.3** Let $R$ be a ring. $a \in R$ is called a left zero divisor if $ab=0$ for some $b \in R$. A <u>zero divisor</u> is an element that is both a left and right zero divisor.

**Ex** 2 is a zero divisor in $\mathbb{Z}_6$.

**Ex** $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is also a zero divisor in $M_2(\mathbb{R})$

since $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

**Def 1.4** Let $R$ be a ring with 1. $a \in R$ is called <u>left invertible</u> if there exists $b \in R$ with $ba=1$. An element that is both left and right invertible is called a <u>unit</u>. The group of units is (usually) denoted $R^*$.

**Ex** $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$ is a unit (since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$)

**Def 1.5** A commutative ring with $1 \neq 0$ and no zero divisors is called an <u>integral domain</u>. A ring with $1 \neq 0$ in which every nonzero element is a unit is called a <u>division ring</u>. A commutative division ring is called a <u>field</u>.

**Ex** $\mathbb{Z}$ is an integral domain.

**Def 1.7** Let $R, S$ be rings. A function $f: R \to S$ is called a <u>homomorphism</u> if

$$f(a+b) = f(a) + f(b) \qquad \text{for all } a, b \in R.$$
$$f(ab) = f(a) f(b)$$

**Def 1.8** Let $R$ be a ring. If there is a least positive integer $n$ s.t. $na=0$ for all $a \in R$, $n$ is called the <u>characteristic</u> of $R$, written $\operatorname{char} R = n$. Otherwise, say $R$ has characteristic 0.

**Ex** $\operatorname{char} \mathbb{Z}_n = n$

**Thm 1.9** Let $R$ be a unital ring with char $R = n > 0$

(i) Let $\varphi: \mathbb{Z} \to R$ be the map given by $\varphi(m) = m \cdot 1$.

$\varphi$ is a homomorphism with ~~kernel~~ $\operatorname{Ker} \varphi = \langle n \rangle$

(ii) $n$ is the least positive integer such that $n \cdot 1 = 0$

(iii) If $R$ has no zero divisors, then $n$ is prime.

**Pf** (i) If $m \in \operatorname{Ker} \varphi$, $ma = m \cdot 1 \cdot a = 0 \cdot a = 0$ for all $a \in R$.

By assumption, $m \geq n$. Write $m = kn + r$ for some $0 \leq r < n$.

Then $ra = 0$ for all $a \in R$, so $r = 0$, i.e. $m \in \langle n \rangle$.

(ii) If $k \cdot 1 = 0$, then $k \cdot a = k \cdot 1 \cdot a = 0a = 0$ for all $a \in R$.

(iii) Suppose $n = kr$ for some $k, r \in \mathbb{N}$.

Then $0 = n \cdot 1 = kr \cdot 1 = k1 \cdot r \cdot 1$ $\boxed{/\!/}$

## §2 Ideals

Observe: If $x, y \in \operatorname{Ker} \varphi$, $x + y, xy \in \operatorname{Ker} \varphi$

But also If $a \in R$, $x \in \operatorname{Ker} \varphi$, $ax \in \operatorname{Ker} \varphi$

**Def 2.1** Let $R$ be a ring. A subring is a subset that is itself a ring.

An left ideal $I$ is a subring satisfying if $x \in R$, $a \in I$, $xa \in I$

A right ideal $I$ is a subring satisfying if $a \in I, x \in R$, $ax \in I$

A (two-sided) ideal is a subring that is both a left and right ideal.

**Ex** $\langle n \rangle$ is an ideal of $\mathbb{Z}$

**Ex** Let $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$. This is a left-sided ideal but not a right ideal.

**Ex** For any ring $R$, $\{0\}$ and $R$ are ideals
$\overset{\shortparallel}{0}$

**Cor 2.3** The intersection of ideals is an ideal.

**Def 2.4** Let $X \subset R$ be a subset. Let $\{A_i\}_{i\in I}$ be the collection of all ideals containing $X$.
Then $(X) = \bigcap_{i\in I} A_i$ is called the <u>ideal generated by $X$</u>.

If $X = \{x_1, \dots, x_n\}$, we write $(x_1, \dots, x_n)$ and say it is <u>finitely generated</u>.

A <u>principal ideal</u> is an ideal generated by a single element.

A <u>principal ideal domain</u> (PID) is an integral domain in which all ideals are principal.

**Ex** In $\mathbb{Z}$, $(3) = \langle 3 \rangle = 3\mathbb{Z}$

**Ex** $\mathbb{Z}$ is a PID. $(a,b) = (d)$ where $d = \gcd(a,b)$, since $d = ma+nb$ for some $m,n \in \mathbb{Z}$.

**Thm 2.6** Let $I, J$ be (left) ideals of a ring $R$.
(i) $I + J = \{x+y \mid x \in I, y \in J\}$ is a (left) ideal
(ii) $IJ = \{\sum x_i y_i \mid x_i \in I, y_i \in J\}$ is a (left) ideal.

**Thm 2.7** Let $R$ be a ring, $I$ an ideal. Then the additive quotient group $R/I$ is a ring with multiplication $(a+I)(b+I) = ab+I$

**Pf** well defined: Suppose $a+I = a_0+I$, $b+I = b_0+I$
$a = a_0 + x$ for some $x \in I$ $\quad b = b_0 + y$ for some $y \in J$

Then $a_0b_0+I = (a-x)(b-y)+I = ab - \underset{\underset{I}{\Uparrow}}{ay} - \underset{\underset{I}{\Uparrow}}{xb} + \underset{\underset{I}{\Uparrow}}{xy} + I = ab + I$. ∎

**Thm 2.8** If $\varphi: R \to S$ is a ring homomorphism, $\operatorname{Ker}\varphi$ is an ideal

**Pf** If $a, b \in \operatorname{Ker}\varphi$, $\varphi(a+b) = \varphi(a)+\varphi(b) = 0+0 = 0$, so $a+b \in \operatorname{Ker}\varphi$

If $a \in \operatorname{Ker}\varphi$, $x \in R$, $\varphi(ax) = \varphi(a)\varphi(x) = 0\varphi(x) = 0$, so $ax \in \operatorname{Ker}\varphi$

$\varphi(xa) = \varphi(x)\varphi(a) = \varphi(x)0 = 0$, so $xa \in \operatorname{Ker}\varphi$ ∎

**Thm 2.9 (First Isomorphism Theorem)** Let $\varphi: R \to S$ be a ring homomorphism.
Then $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$

**Pf** Let $\bar{\varphi}: R/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$, $a + \operatorname{Ker}\varphi \mapsto \varphi(a)$ be the well defined abelian group isomorphism.

Check: $\bar{\varphi}(a+\operatorname{Ker}\varphi)\bar{\varphi}(b+\operatorname{Ker}\varphi) = \varphi(a)\varphi(b) = \varphi(ab)$

$\bar{\varphi}(ab+\operatorname{Ker}\varphi) = \varphi(ab)$  so $\bar{\varphi}$ is a ring isomorphism. ∎

**Thm 2.13** Let $I \subset R$ be an ideal. There is a one-to-one correspondence between ideals of $R/I$ and ideals of $R$ containing $I$.

**Def** A *prime ideal* $P$ of a ring $R$ is a proper ideal satisfying

$IJ \subset P \Rightarrow I \subset P$ or $J \subset P$   for all ideals $I, J \subset R$

**Thm 2.15** Let $P$ be a proper ideal of a ring $R$.

1) If $R \setminus P$ is multiplicatively closed, then $P$ is prime.
2) If $R$ is commutative and $P$ is prime, then $R \setminus P$ is multiplicatively closed.

**Remark** $R \setminus P$ multiplicatively closed $\Leftrightarrow$ If $a, b \in R$ with $ab \notin P$, either $a \notin P$ or $b \notin P$

<u>Pf</u> (i) Let $I, J \subset R$ be ideals with $IJ \subset P$.

Suppose $I \not\subset P$ (so we will show $J \subset P$).

Let $x \in I \setminus P$. Let $y \in J$.

Then $xy \in IJ \subset P$, so $y \in P$ (since $x \notin P$).

This holds for all $y \in J$, so $J \subset P$.

(ii) Let $a, b \in R$ with $ab \in P$

<u>Claim</u> $(a)(b) \subset P$

If $x \in (a)(b)$, $x = ar_1 br_2$ for some $r_1, r_2 \in R$
$= (ab) r_1 r_2 \in P$.

$P$ prime $\Rightarrow$ $(a) \subset P$ (so $a \in P$) or $(b) \subset P$ (so $b \in P$)

<u>Cor</u> Let $R$ be a commutative unital ring. Then $(0)$ is prime iff $R$ is an integral domain.

<u>Pf</u> Let $a, b \in R \setminus (0)$. Then $(0)$ is prime iff $ab = 0$ implies $a = 0$ or $b = 0$ iff $R$ is an integral domain. $\square$

<u>Ex</u> The prime ideals of $\mathbb{Z}$ are precisely $(p)$ for primes $p$.

<u>Thm 2.16</u> Let $R$ be a commutative, unital ring. An ideal $P$ is prime iff $R/P$ is an integral domain.

<u>Pf</u> $\Rightarrow$ Let $a+P, b+P \in R/P$.
If $(a+P)(b+P) = 0+P$, $ab + P = P$, i.e. $ab \in P$.
Then $a \in P$ or $b \in P$, so $a + P = 0 + P$ or $b + P = 0 + P$
Thus $R/P$ is an integral domain.

$\Leftarrow$ Suppose $R/P$ is an integral domain. Let $a, b \in R$ with $ab \in P$.
Then $(a+P)(b+P) = 0 + P$, so $a + P = 0 + P$ or $b + P = 0 + P$
i.e. $a \in P$ or $b \in P$.

Thus $P$ is prime ■ $\square$

**Def 2.17** Let $R$ be a ring. A proper ideal $M$ is called <u>maximal</u> if it is not contained in any other proper ideal.

**Ex** $(3)$ is maximal in $\mathbb{Z}$. $(6)$ is not maximal since $(6) \subset (2)$.

**Thm 2.18** Let $R$ be a unital ring. Then $R$ contains a maximal ideal. Moreover, every proper ideal is contained in some maximal ideal.

**Pf** Let $\mathcal{P}$ be the poset of proper ideals of $R$ ordered by inclusion.

Let $\mathcal{C} = \{ C_i \mid i \in I \}$ be a chain of proper ideals

<u>Claim</u> $C := \bigcup_{i \in I} C_i$ is an upper bound for $\mathcal{C}$

(1) $C$ is a proper ideal: Let $a, b \in C$, so $a \in C_i$, $b \in C_j$.

Since $\mathcal{C}$ is a chain, WLOG $C_i \subset C_j$, so $a+b, ab \in C_j \subset C$.

If $r \in R$, $ra \in C_i \subset C$.

Note $1 \notin C_i$ for all $i \in I$, so $1 \notin C$.

(2) $C_i \subset C$ for all $i \in I$: By construction.

Then Zorn $\Rightarrow$ $\mathcal{P}$ has a maximal element. ☒

**Thm 2.19** Let $R$ be a commutative unital ring. Every maximal ideal is a prime ideal

**Pf** Let $M$ be a maximal ideal, and $a, b \in R \setminus M$.

Then $M + (a) = M + (b) = R$, so

$1 = m_1 + ar_1 = m_2 + br_2$ for some $m_1, m_2 \in M$, $r_1, r_2 \in R$.

Then $1 = (m_1 + ar_1)(m_2 + br_2) = \underbrace{m_1 m_2 + m_1 b r_2 + m_2 a r_1}_{M} + ab r_1 r_2$

If $ab \in M$, then $1 \in M$ ↯ so $ab \notin M$, thus $M$ is prime. ☒

**Thm 2.20** Let $R$ be a unital ring.

(i) If $R/M$ is a division ring, then $M$ is maximal.

(ii) If $R$ is commutative, then $M$ is maximal $\iff R/M$ is a field.

**Pf** (i) Let $N$ be an ideal with $M \subsetneq N$.

Let $a \in N \setminus M$. Then there exists $b \in N \setminus M$ with $(a+M)(b+M) = 1+M$

so $ab - 1 \in M \subset N$. But $ab \in N$, so $1 \in N$, i.e. $N = R$.

Thus $M$ is maximal.

(ii) $\Leftarrow$ Follows from (i)

$\Rightarrow$ Suppose $M$ is maximal. Then $M$ is prime, so $R/M$ is an integral domain.

Let $a+M \neq 0+M$, (so $a \notin M$).

Then $(a)+M = R$, so $1 = ar+m$ for some $r \in R$, $m \in M$.

Then $(a+M)(r+M) = ar+M = 1+M$

Thus every ~~elect~~ nonzero element of $R/M$ has a multiplicative inverse,

So $R/M$ is a field.

**Cor 2.21** Let $R$ be a commutative unital ring. TFAE

(i) $R$ is a field

(ii) $R$ has exactly two ideals, $0$ and $R$:

(iii) $0$ is a maximal ideal

(iv) Every nonzero homomorphism of rings $R \longrightarrow S$ is injective.

**Pf** Thm 2.20 gives ~~(i)~~ (i) $\iff$ (iii). Clearly (ii) $\iff$ (iii)

(iv) $\iff$ Either $\ker \varphi = 0$ or $\ker \varphi = R$ $\iff$ (ii) ∎

**Thm 2.22, 2.23** Let $\{R_i\}_{i\in I}$ be a collection of rings. Then $\prod_{i\in I} R_i$ is a ring (with component wise multiplication) that is ~~the~~ a product in the category of rings.

**Thm 2.24** Let $R$ be a ring, $I_1, \dots, I_n \subset R$ ideals. Suppose

(i) $I_1 + \dots + I_n = R$

(ii) $I_k \cap (I_1 + \dots + I_{k-1} + I_{k+1} + \dots + I_n) = 0$ for each $1 \le k \le n$.

Then $R \cong I_1 \times \dots \times I_n$.

Pf $\varphi: I_1 \times \dots \times I_n \longrightarrow R$ given by $\varphi(x_1, \dots, x_n) = x_1 + \dots + x_n$ is an abelian group isomorphism.

Observe: If $x \in I_i$, $y \in I_j$, then $xy \in I_i \cap I_j = 0$

Let $(a_1, \dots, a_n), (b_1, \dots, b_n) \in I_1 \times \dots \times I_n$

then
$$\varphi(a_1, \dots, a_n)\varphi(b_1, \dots, b_n) = (a_1 + \dots + a_n)(b_1 + \dots + b_n)$$
$$= a_1 b_1 + \dots + a_n b_n$$
$$= \varphi((a_1, \dots, a_n)(b_1, \dots, b_n))$$ ∎

**Thm 2.25** ("Chinese Remainder Theorem" – Sun-Tsze, ~400 AD)

Let $I_1, \dots, I_n \subset R$ be ideals such that $R^2 + I_i = R$ for all $i$ and $I_i + I_j = R$ for all $i \neq j$ ($I_1, \dots, I_n$ called pairwise comaximal)

Let $b_1, \dots, b_n \in R$. Then there exists $b \in R$ such that
$$b \equiv b_i \bmod I_i \quad \text{for each } 1 \le i \le n.$$

Moreover, $b$ is uniquely determined up to congruence modulo $I_1 \cap \dots \cap I_n$