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

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

□

Chapter 1

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

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

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

Remark Identity and inverses must be unique

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

Ex Classify as semigroup / monoid / group : $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ (under $+$)
$\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Z}\setminus\{0\}$, $\mathbb{Q}$, $\mathbb{Q}\setminus\{0\}$ (under $\cdot$)

Prop 1.3 Let G be a semigroup. Then G is a group if and only if left* inverses exist and a left* identity exists, i.e.
(i) there exists $e \in G$ s.t. $ex = x$ for all $x \in G$
(ii) for each $x \in G$, there exists x^{-1} s.t. $x^{-1}x = e$.

Remark Also true for "right".

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

Ex Symmetric group

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

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

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

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

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

— x —

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

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

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

Ex If A is an abelian group, the map $a \longmapsto a^{-1}$ is an automorphism.
The map $a \longmapsto a^2$ 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 $\iff$ $\ker f = \{e\}$

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

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, id, + inverses.

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

Ex $\{1, r, r^2, r^3, \ldots r^{n-1}\}$ 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 $$\langle X \rangle = \{ a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \mid a_i \in X, n_i \in \mathbb{Z} \}$$

— 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 $\mathbb{Z}_n$.

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 $|G| = n$, then $\langle a^k \rangle = G \iff (k, n) = 1$

— x —

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

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

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

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

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

Thm 4.2 (i) These are equivalence relations

(ii) The equivalence classes are the right (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 $a, b \in G$ $\quad Ha = Hb \iff ab^{-1} \in H$

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

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

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 $|I| = [G:H]$

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

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

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

$b_j a_i \in Ha_i$ since $b_j \in H$; $k b_r a_t \in Ha_t$ since $kb_r \in H$

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

then $b_j = k b_r$, 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 $|a| \mid |G|$ for all $a \in G$.

Notation Let G be a group, H, K subsets of G.

$$HK = \{ab \mid a \in H, b \in K\}$$

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

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

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

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

Claim $HK = Hk_1 \amalg Hk_2 \amalg \dots \amalg Hk_n$

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

Pf of claim Need to show

(1) HK_i and HK_j are disjoint

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

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

(1) Suppose $h_i K_i = h_j K_j$

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

$\Rightarrow K_j \in CK_i \Rightarrow K_j = K_i$

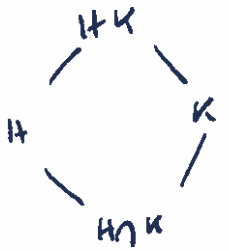
(2) Let $hk \in HK$ $(h \in H, k \in K)$

Then $k = ck_i$ for some i, $c \in C$.

Then $hk = (hc)k_i \in HK_i$ ∎

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



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. $h_1 h_2^{-1} \in H\cap K \leq K$, 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 $(H\cap K)h_1 = (H\cap K)h_2$ ∎

Prop 4.9 Let G be a group, $H, K \leq G$ s.t. HK is a subgroup
If H, K are finite index in HK, then $[HK : H \cap K] = [HK : H][HK : K]$

Pf Thm 4.5 + Prop 4.8 ☐

— x —

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

(i) Left cosets are right cosets

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

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

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

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

Pf (i) $\Rightarrow$ (ii) Let aN be a left coset. Then $aN = Nb$ for some $b \in G$.
In particular, $a \in Na \cap Nb \Rightarrow Na = Nb$. So $aN = Na$.

(ii) $\Rightarrow$ (iii) Immediate.

(iii) $\Rightarrow$ (iv) Immediate

(iv) $\Rightarrow$ (i) Let aN be a left coset.
If $b \in N$, $aba^{-1} \in N$, so $ab \in Na \Rightarrow aN \subseteq Na$.
Similarly, $Na \subseteq aN$. ☐

Ex In an abelian group, all subgroups are normal!

Ex Recall $D_{8} = \langle r, s \mid r^4 = 1, s^2 = 1, srs = r^{-1} \rangle$

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

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

Remark: If $N \trianglelefteq G$ 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) $N \trianglelefteq \langle N, K \rangle$ (book uses notation NVK)

(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 a subgroup, $NK = KN$ (homework)

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

Let $n_1 k_1 n_2 k_2 \dots n_r k_r \in \langle N, K \rangle$ $(n_i \in N, k_i \in K)$

Induct on r: If $r = 1$, $n_1 k_1 \in NK$

If $r > 1$: Assume $n_1 k_1 \dots n_{r-1} k_{r-1} = n_0 k_0 \in NK$

$$n_1 k_1 \dots n_{r-1} k_{r-1} n_r k_r = n_0 k_0 n_r k_r$$
$$= \underbrace{n_0 (k_0 n_r k_0^{-1})}_{N} \underbrace{k_0 k_r}_{K} \in NK.$$

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

Thm 5.4 Let G be a group, $N \trianglelefteq G$. 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 $\tilde{a} = an_1$ $\quad \tilde{b} = bn_2$

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

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

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

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

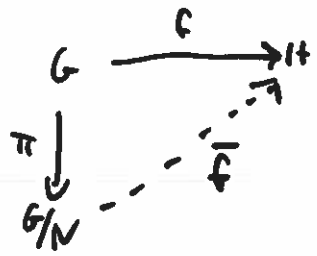
Thm 5.5 (i) If $f: G \to H$ is a group hom., then $\ker f \trianglelefteq G$.
(ii) If $N \trianglelefteq G$, then $\pi: G \to G/N$ is a (surjective) hom with $\ker \pi = N$
$\pi(a) = aN$.

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

(ii) 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

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

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



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

↳ write $a = bn$ for some $n \in N$.

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

↑ since $N \trianglelefteq \ker f$

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

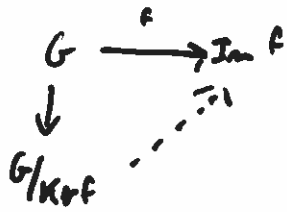
$\bar{f}(aN\,bN) = \bar{f}(abN) = f(ab)$

$\bar{f}(aN)\bar{f}(bN) = f(a)f(b)$ ∎

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

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

Pf



Surjective by construction
Injective by remark

∎

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

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

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

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

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

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 $a \in N \Rightarrow a \in N\cap K$.

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

Since $N\cap K = \ker\varphi$, $\bar\varphi$ is injective.

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

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

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

$\Rightarrow \bar\varphi$ is an isomorphism. ∎

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 $\dfrac{G/K}{H/K} \cong G/H$

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

$$\begin{array}{ccc} G & \longrightarrow & G/H \\ \downarrow & \nearrow_{\bar\varphi} & \\ G/K & & \end{array}$$

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

Suppose $aK \in \ker\bar\varphi$, so $\bar\varphi(aK) = H$

$\Leftrightarrow aH = H$, iff $a \in H$. Thus $H/K = \ker\bar\varphi$

∎

—x—

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

* Can permute the cycles

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

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

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

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

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

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

(In general: odd length cycles are even)

Thm 6.7 A permutation cannot be both even & odd.

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

Suppose $\sigma_1 \dots \sigma_s = \tau_1 \dots \tau_r$

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 on r

Products of transpositions:

$(ab)(ab) = id$

$(ab)(cd) = (cd)(ab)$

$(ab)(ac) = (bc)(ab)$

$(ab)(bc) = (bc)(ac)$

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

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

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

Exercise It is the only subgroup of index 2 ∎

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

Def A group G is called <u>simple</u> if it has no proper normal subgroups

Ex $\mathbb{Z}_p$ for prime p are precisely the simple abelian groups

Thm 6.10 A_n is simple if and only if $n \neq 4$

Lemma $\sigma(x_1 x_2 \dots x_r)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2) \dots \sigma(x_r))$

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 <u>S_n</u>

i.e. If τ_1, τ_2 are 3-cycles $\tau_1 = \sigma \tau_2 \sigma^{-1}$ for some $\sigma \in S_n$

If σ is odd: choose 2 elements a, b not appearing in τ_2

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

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

$= \tau_1$ ∎

Lemma Let $n \geq 5$. If $N \trianglelefteq A_n$ and N contains a 3-cycle, then $N = A_n$

Pf It suffices to show that A_n is generated by 3-cycles

Claim A product of two transpositions is generated by 3-cycles.

Pf Case 1 $(ab)(cd) = (acb)(acd)$

Case 2 $(ab)(ac) = (acb)$

Case 3 $(ab)(ab) = id.$ ∎

Pf of Thm 6.10 Suppose $H \trianglelefteq A_n$ 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 $\sigma = (123\ldots r)\tau$

Let $\delta = (123)$

$H \ni \sigma^{-1}\delta\sigma\delta^{-1} = \tau^{-1}(r\ldots321)(123)(123\ldots r)\tau(321)$

$= (1\ 3\ r)$

Case 2 Multiple 3-cycles

WLOG $\sigma = (123)(456)\tau$

Let $\delta = (124)$

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

$= (1\ 4\ 2\ 6\ 3)$

Apply Case 1

Case 3 Single 3-cycle

WLOG $\sigma = (123)\tau$

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

Case 4 Product of transpositions

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

Let $\delta = (123)$

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

$= (13)(24)$

Call this $\sigma_0 \in H$

Let $\delta_0 = (135)$

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

$= (135)$ ☑

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

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

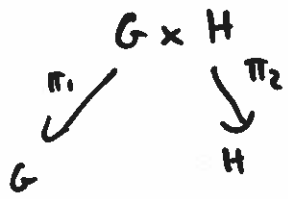
with operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

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

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

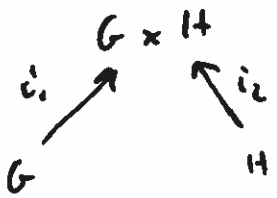
Fact $|G \times H| = |G|\,|H|$

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 $\ker \pi_1 = i_1(G) \cong G$ $\qquad$ $G \times H / G \cong H$

$\ker \pi_2 = i_2(H) \cong H$ $\qquad$ $G \times H / H \cong G$

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

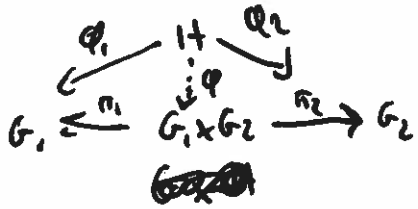
Def Let $\{G_i\}_{i \in I}$ be a collection of groups.

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 $\varphi_1 : H \to G_1$, $\varphi_2 : H \to G_2$.

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



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

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

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

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

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

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 $N \trianglelefteq G$, $H \leq G$. The TFAE:

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

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

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

(4) There exists a split exact sequence

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

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

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

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

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

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

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

(3) $\Rightarrow$ (4) $\quad 1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$, with σ going back from H to G

α = inclusion (injective)

σ = inclusion

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

Is β a homomorphism?

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

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

$$\beta(h_1n_1h_2n_2) = \beta(h_1h_2\underbrace{h_2^{-1}n_1h_2n_2}_{\in N}) = h_1h_2 = \beta(h_1n_1)\beta(h_2n_2)$$

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

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

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

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

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

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

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

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

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

$= e$

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 $x \in \alpha(N)$, $\quad e = \beta(x) = \beta\sigma(y) = y$, $\quad$ so $x = \sigma(e) = e$ ☑

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

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

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

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

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

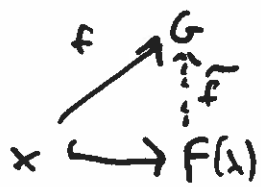
$(x, y, x, x, x^{-1}, y, y, 1, 1, 1, \dots)$ is a word (Think: $xyxxx^{-1}yy$)

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

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

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

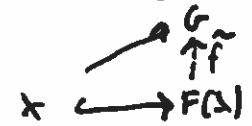
Thm 9.2 The free group is a free object in the category of groups.
In other words, if $f: X \longrightarrow G$ is a map of sets from a group G,
then is a unique homomorphism $\tilde{f}: F(X) \to G$



Pf Define $\tilde{f}(x_1^{n_1} \cdots x_r^{n_r}) = f(x_1)^{n_1} \cdots f(x_r)^{n_r}$

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

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



∎

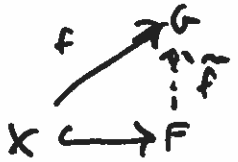
Thm-Def 1.1 Let F be an abelian group. TFAE

(i) F has a nonempty <u>basis</u>, i.e. a generating set X s.t.
whenever $n_1x_1 + \cdots + n_kx_k = 0$ for $n_i \in \mathbb{Z}$, $x_i \in X$, then $n_i = 0$ for all i.
(Thm: 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 $\tilde{f}: F \to G$



Pf (i) $\Rightarrow$ (ii) If ~~$x \in X$~~ $x \in X$, 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, $n x_0 = n_1 x_1 + \cdots + n_r x_r$ for some $n, n_i \in \mathbb{Z}$, $x_i \in X$
Thus, $F = \bigoplus_{x \in X} \langle x \rangle$

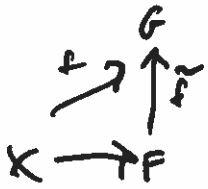
(ii) $\Rightarrow$ (iii) $\mathbb{Z}$ is the only infinite cyclic group.

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

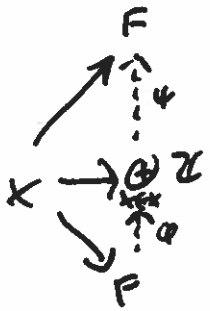
Define $\tilde{f}: F \to G$ by $\tilde{f}(\sum n_i x_i) = \sum n_i f(x_i)$



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

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

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



Uniqueness $\Rightarrow \psi\varphi = id$

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.

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

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

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

Thus φ is surjective.

Suppose $y = a_1 x_1 + \dots + a_n x_n \in \ker \varphi$ WLOG $a_i \neq |x_i|$

Let $\sigma_i : C_1 \oplus \dots \oplus C_n \to C_i$ be the i^{th} 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 φ is injective

∎

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

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

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

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

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

Then $\langle a \rangle \oplus \langle b \rangle$ is a subgroup of order ab, which 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 **action** is a map

$$G \times S \longrightarrow S \qquad (g, x) \longmapsto g \cdot x$$

such that for all $x \in S$, $g_1, g_2 \in G$

1) $e \cdot x = x$
2) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$

we say **G acts on S**, 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 $\mathbb{R}^n$ 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

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

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 **orbits** (sometimes written $G\cdot x$)

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 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 **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 $|G| = \sum_{i=1}^{\hat{}} [G : C_G(x_i)]$

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

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

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

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

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

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

(is isomorphic to a subgroup of)

Cor 4.6 (Cayley's Thm) Let G be a group. Then G embeds in a symmetric group.

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

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

Compute $\ker \varphi$: Suppose $\varphi(g) = id$

$\varphi(g) = \mathcal{T}_g$

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

$g \cdot x = gx$

i.e. $g = e$.

Thus $\ker \varphi = \langle e \rangle$, 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 $G \longrightarrow \mathrm{Aut}\, G$ whose kernel is the center of G $\quad C(G) = \{ g \in G \mid gx = xg \text{ for all } x \in G \}$.

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

(ii) $\gamma_g \gamma_h = \gamma_{gh}$, so the map $G \longrightarrow \mathrm{Aut}G$, $g \longmapsto \tilde{\gamma}_g$ 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 $\varphi: G \to S(\{gH\})$ is contained in H.

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

"

$\tilde{\gamma}_g$

Then $\tilde{\gamma}_g(H) = H$

"

$g \cdot H$

"

gH $\Rightarrow$ $g \in H$. ∎

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 $G \longrightarrow S(\{gH\})$ 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 $G \longrightarrow S(X) \cong S_p$

$K \trianglelefteq G$, 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 $|G/K| = [G:K] = [G:H][H:K] = p[H:K]$ Typo

Thus $\not\exists$ $|G/K| = p$ and $[H:K] = 1$, i.e. $K = H$.

But K was normal in G. ∎

Motivation: 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 $|S| \equiv |S_0| \bmod p$

Pf $S = S_0 \amalg H \cdot x_1 \amalg H x_2 \amalg \cdots \amalg H \cdot x_r$

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

↑ 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 $\langle (1\,2\,3 \cdots p) \rangle \leq S_p$ 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, $\because (e, \ldots, e) \in S_0$,

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

S_0 non-phy $\Rightarrow |S_0| > 1$, 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 $\langle 37 \rangle$ 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 $\Rightarrow q = p$. ∎

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: $|G| = |Z(G)| + \sum [G : C_G(x)]$

(each term divides $|G| = p^n$)

Thus $p \mid |Z(G)|$ ∎

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

Pf Let S be set of left cosets of H

H acts on S by left translation

what are fixed points?

$xH \in S_0 \iff hxH = xH$ for all $h \in H$

$\iff x^{-1}hx \in H$ for all $h \in H$

$\iff x^{-1}Hx = H$

$\iff x \in N_G(H)$

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 $|S| = [G:H]$ ☐

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

pf By lemma, $[N_G(H) : H] \equiv [G:H] \bmod p \equiv 0 \bmod p$.

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

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 ($i < n$) is normal in some subgroup of order p^{i+1}.

pf

Claim If $H < G$ is a subgroup of order p^i ($1 \leq i < n$), then 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 $H \leq G$, and $|H| = p^i$ for $1 \leq i < n$

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

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

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

(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 $H_1 \leq N_G(H)$).

$H \trianglelefteq H_1$, 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 $\Rightarrow$ $|S_0| \equiv [G:P] \bmod p$.

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,

Orbit stabilizer $\Rightarrow$ $r = [G : N_G(P_1)]$ which must divide $|G|$.

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 $P_i \trianglelefteq N_G(P_i)$

$\Rightarrow P_i = P_1$.

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

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 $p \equiv 1 \bmod q$)

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 $N \cap H = \langle e \rangle$.
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
$p = r \equiv 1 \bmod q$ ∎

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 $H \cap N = \langle e \rangle$, and $|HN| = |H||N| = 4 \cdot 2 = 8 = |G|$, so $HN = G$.
Thus $G \cong N \rtimes H = \mathbb{Z}_4 \rtimes \mathbb{Z}_2 = D_8$

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) $bab^{-1} = e \Rightarrow a = e$ ↯

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

(iii) $bab^{-1} = a^2 \Rightarrow ba^2b^{-1} = e \Rightarrow a^3 = e$ ↯

(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 $\ker \varphi \trianglelefteq P$

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

$\Rightarrow G \cong P \rtimes K$

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 Issues) del Ferro, Tartaglia, Cardano

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

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

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

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

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

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

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

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

Quadratic in w^3!

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

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

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

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

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

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

(3) $s = lm$

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

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

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

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

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

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

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

$0 = K^6 + 2qK^4 + (q^2 - 4s)K^2 - r^2$ (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 $\mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right)$

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

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

∎

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

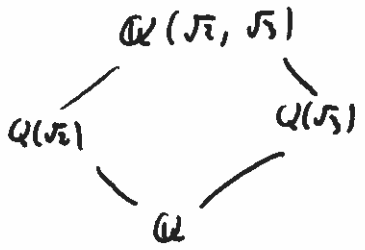
If $f \in k[x]$, the Galois group of f is the Galois group of its splitting field over k.

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

Pf By Thm V.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 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q})$

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

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

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

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

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

Thm A (V.2.5) Let p be prime, k a field containing a primitive p^{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 α be a root. Then all of the roots are $\{\alpha, \omega\alpha, \omega^2\alpha, \dots, \omega^{p-1}\alpha\}$ for a primitive root of unity ω.

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 $\{\alpha, \omega\alpha, \dots, \omega^{p-1}\alpha\}$. 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 σ

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. ∎

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

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

Pf Define $\mathfrak{D}: \mathrm{Gal}(E/k) \longrightarrow \mathrm{Gal}(K/k)$

$\sigma \longmapsto \sigma|_K$

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

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

Thm V.9.11 Let $f \in \mathbb{k}[x]$ have degree n. Assume $\mathbb{k}$ contains p^{th} roots of unity for $p \le n$. Let E be the splitting field of f over $\mathbb{k}$. If f is solvable by radicals, then there exist subgroups $G_i \le G := Gal(E/\mathbb{k})$ such that

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

(ii) $G_{i+1} \trianglelefteq G_i$

(iii) G_i / G_{i+1} is cyclic of prime order for all i.

Pf Since f is solvable by radicals, there exist fields

$$\mathbb{k} = K_0 \subset K_1 \subset \cdots \subset K_t$$

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 β_{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 $\Rightarrow$ Each K_{i+1} is a splitting field

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

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