

A PRECIS ON A SUMMER OF GROUP THEORY.¹

Contents (in order of appearance)

- Group actions and Sylow theorems.
- Isomorphism theorems.
- Group presentations.
- Finitely-generated abelian groups.
- Alternating groups.
- Composition series and the Jordan-Hölder theorem.
- Solvable groups.

References

- Sue Sierra. Group Theory. University of Edinburgh. 2020.
- J. J. Rotman. An Introduction to the Theory of Groups. Springer New York, NY. 1994.
- Ahmed Ayache, Khalid Amin. Introduction to Group Theory. Springer Singapore. 2025.
- David S. Dummit, Richard M. Foote. Abstract Algebra, 3rd edition. Wiley. 2003.

¹Version of 2025/07/28. Notes taken by David Punton.

A group $(G, *)$ is a set G equipped with an associative map $*$: $G \times G \rightarrow G$ so that G has an identity and inverses with respect to $*$. If $*$ is commutative, then G is abelian. A subgroup H of a group G is a nonempty subset $H \subseteq G$ which is closed under $*$ and taking inverses, and is denoted $H \leq G$. For any subgroup $H \leq G$, then $e_H = e_G$ and inverses in H and G are identical.

Subgroup test.

If G is a group and $H \subseteq G$, then $H \leq G$ iff H is nonempty and $xy^{-1} \in H$ for all $x, y \in H$.

The subgroup of a group G generated by a nonempty set $X \subseteq G$ is

$$\langle X \rangle := \{x_1^{a_1} x_2^{a_2} \cdots x_k^{a_k} \mid a_i \in \{\pm 1\}, x_i \in X \text{ for all } 1 \leq i \leq k, k \geq 0\}$$

and can equivalently be characterised as the intersection of all subgroups of G which contain X . In this sense, $\langle X \rangle$ is the ‘smallest’ subgroup of G which contains X . A group G is finitely generated if there exists a finite set $X \subseteq G$ such that $G = \langle X \rangle$. A group G is cyclic if there exists $g \in G$ such that $G = \langle \{g\} \rangle := \langle g \rangle$.

The order of a group G is the number of elements of the group, and is denoted $|G|$. If G contains infinitely many elements, then $|G| := \infty$. The order of an element $a \in G$ is the order of $\langle a \rangle \leq G$.

The cyclic group of order $n \in \mathbb{Z}_{>0}$ is $C_n := \langle g \mid g^n = e \rangle$. (Strictly speaking, I’m cheating here: this is a group presentation of C_n which we’ll see later.)

Let G be a group and $H \leq G$. A left coset of H in G is $gH := \{gh : h \in H\}$ for some $g \in G$. A right coset of H in G is $Hg := \{hg : h \in H\}$ for some $g \in G$. There is an equivalence relation on G given by $g_1 \sim g_2$ iff $g_1 \in g_2 H$ for all $g_1, g_2 \in G$. An analogous equivalence relation exists on G for right cosets of H in G .

Lagrange’s theorem.

If G is a group and $H \leq G$, then $|G| = [G : H]|H|$ where $[G : H]$ is the *index*, meaning the number of left (or equivalently, right) cosets, of H in G .

GROUP ACTIONS AND SYLOW THEOREMS.

The converse of Lagrange’s theorem doesn’t generally hold, but there exist partial converses, such as:

Cauchy’s theorem.

If G is a group and p is a prime which divides $|G|$, then there exists $H \leq G$ such that $|H| = p$.

A p -group is a group in which every element is of order p^k . A p -subgroup is a subgroup which is a p -group. A finite group G is a p -group if and only if $|G| = p^k$ for some $k \in \mathbb{Z}$.

A left group action of a group G on a set X is a map $\alpha : G \times X \rightarrow X$ such that $\alpha(e, x) = x$ and $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ for all $g, h \in G$ and $x \in X$. A right group action is defined analogously. It’s common to write $g.x := \alpha(g, x)$ for a group action α , $g \in G$ and $x \in X$. Given a group action, the orbit of an element $x \in X$ is $G.x := \{g.x : g \in G\} \subseteq X$ and the stabiliser of $x \in X$ is $\text{Stab}_G(x) := \{g : g.x = x\} \subseteq G$. A fixed point of a group action is $x \in X$ such that $G.x = \{x\}$.

If G is a finite group which acts upon a set X , then $\text{Stab}_G(x) < G$ for each $x \in X$. Moreover, there exists an equivalence relation \sim on X such that for all $x, y \in X$, $x \sim y$ iff there exists $g.x = y$. That is, a group action partitions a set into orbits. Lastly, we have:

Orbit-stabiliser theorem.

If G is a finite group which acts on a set X , then $|G| = |G.x| |\text{Stab}_G(x)|$ for all $x \in X$.

A pair of elements $a, b \in G$ are conjugate if there exists $g \in G$ such that $a = bgb^{-1}$. A group G acts on itself by conjugation via the map $G \times G \rightarrow G$, $(g, a) \mapsto gag^{-1}$. The conjugacy class $\text{Cl}(a)$ of an element $a \in G$ is the orbit of a under conjugation; hence, conjugation partitions a group into conjugacy classes so that the class equation $|G| = \sum_i |\text{Cl}(a_i)|$ for a finite set $\{a_1, \dots, a_k\} \subset G$.

The centraliser $C_G(a)$ of an element $a \in G$ is the stabiliser of a under conjugation, given explicitly as the subset of G with respect to which a is invariant under conjugation, $C_G(a) := \{g : a = gag^{-1}\}$.

Immediately, $C_G(a) < G$. Also, $|G| = |Cl(a)||C_G(a)|$ for each $a \in G$ and thus $|Cl(a)| = [G : C_G(a)]$ by Lagrange's theorem.

A pair of subsets $T, S \subseteq G$ are conjugate if there exists $g \in G$ such that $T = gSg^{-1}$. That is, conjugation by g induces a one-to-one correspondence between T and S . The centraliser $C_G(S)$ of a subset $S \subseteq G$ is $C_G(S) := \{g : s = gsg^{-1} \text{ for all } s \in S\} \leq G$. The centre $Z(G)$ of a group G is $Z(G) := C_G(G)$. The normaliser $N_G(S)$ of a subset $S \subseteq G$ is $N_G(S) := \{g : S = gSg^{-1}\} \leq G$ such that $C_G(S) \subset N_G(S)$.

A subgroup $H \leq G$ is normal if $H = gHg^{-1}$ for all $g \in G$, and is denoted $H \triangleleft G$. Equivalently, $H \triangleleft G$ iff $gHg^{-1} \leq H$ iff $G = N_G(H)$ iff left and right cosets of H in G coincide. Given an arbitrary subgroup $K \leq G$, the normaliser $N_G(K)$ is equal to the union of all subgroups (*i.e.* the 'largest' subgroup) which contain K as a normal subgroup.

Our group action technology and a pair of lemmas, which are:

1. If p is a prime and G is a finite- p group which acts on a finite set X , then the number of fixed points in X is congruent to $|X|$ modulo p ,

2. If G is a finite group and $H \leq G$, then $[G : N_G(H)]$ equals the number of distinct conjugate subgroups of H in G and moreover, for each prime p which divides $|G|$ and Sylow p -subgroup $P \leq G$, we have $n_p = [G : N_G(P)]$,

allow us to prove:

Sylow theorems.

Let G be a group and p be a prime such that k is the largest exponent for which p^k divides $|G|$.

1. There exists a subgroup of G whose order is p^k . Such a subgroup is called a Sylow p -subgroup.

2. For each Sylow p -subgroup $P \leq G$ and p -subgroup $H \leq G$, there exists $g \in G$ such that $H \subseteq gPg^{-1}$. Hence, any two Sylow p -subgroups of G are conjugate.

3. The number n_p of Sylow p -subgroups of G divides $|G|/p^k$, is congruent to 1 modulo p and equals $[G : N_G(P)]$ for each Sylow p -subgroup $P \leq G$.

As a consequence of the Sylow theorems, a Sylow p -subgroup of G is normal iff $n_p = 1$. A subgroup $H \leq G$ is simple if H contains only $\{e\}$ and H as normal subgroups; that is, H contains no 'non-trivial' normal subgroups.

ISOMORPHISM THEOREMS.

Given a pair of groups G and H , a group homomorphism is a map $\phi : G \rightarrow H$ such that for all $g, h \in G$, $\phi(gh) = \phi(g)\phi(h)$. A group isomorphism is a bijective group homomorphism. If $\phi : G \rightarrow H$ is a group homomorphism, then $\phi(e_G) = e_H$ and $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$. The kernel $\ker \phi$ of a group homomorphism $\phi : G \rightarrow H$ is $\ker \phi := \{g : \phi(g) = e_H\} \subseteq G$. A subgroup $N \leq G$ is normal in G iff there exists a group H and a group homomorphism $\phi : G \rightarrow H$ such that $\ker \phi = N$.

A factor group G/N is the set of left (or equivalently, right) cosets of a normal subgroup $N \triangleleft G$ in G equipped with the group operation $(gN) * (hN) = (gh)N$ for each $g, h \in G$. There is a canonical surjective group homomorphism $\text{can} : G \rightarrow G/N, g \mapsto gN$.

Universal property of factor groups.

Let G be a group and $N \triangleleft G$. For each group H and group homomorphism $\psi : G \rightarrow H$ with $N \subseteq \ker \psi$, there exists a unique group homomorphism $\bar{\psi} : G/N \rightarrow H$ such that $\psi = \bar{\psi} \circ \text{can}$.

As a useful corollary, if $\phi : G \rightarrow K$ is a surjective group homomorphism and $\psi : G \rightarrow H$ is a group homomorphism with $\ker \phi \subseteq \ker \psi$, then there exists a unique group homomorphism $\bar{\psi} : K \rightarrow H$ such that $\psi = \bar{\psi} \circ \phi$.

First isomorphism theorem.

If G, H are groups and $\phi : G \rightarrow H$ is a group homomorphism, then $\ker \phi \triangleleft G$, $\text{im} \phi \leq H$ and there exists a group isomorphism $\bar{\phi} : G/\ker \phi \rightarrow \text{im} \phi$ given by $gN \mapsto \phi(g)$ with $N := \ker \phi$. If ϕ is surjective, then $G/\ker \phi \cong H$.

If G is a group and $N \triangleleft G$, then we make two observations: first, if $K \leq G/N$, then $\text{can}^{-1}(K) \leq G$ with $N \subseteq \text{can}^{-1}(K)$ and moreover, $\text{can}^{-1}(K) \triangleleft G$ if and only if $K \triangleleft G/N$; second, if $N \leq H \leq G$, then $H = \text{can}^{-1}(\text{can}(H))$. Combining these allows us to prove:

Correspondence theorem.

Let G be a group, $N \triangleleft G$ and $\text{can} : G \rightarrow G/N$ denote the canonical surjection. There is a bijection between subgroups of G which contain N and subgroups of G/N given by $H \mapsto \text{can}(H)$ which restricts to a bijection between normal subgroups of G which contain N and normal subgroups of G/N .

Furthermore, if $A, B \leq G$, then $A \subseteq B$ iff $\text{can}(A) \subseteq \text{can}(B)$.

which in turn allows us to prove:

Third isomorphism theorem.

If G is a group and $N \leq H \leq G$ are such that $N, H \triangleleft G$, then $(G/N)/(H/N) \cong G/H$.

Given a pair of subsets $X, Y \subseteq G$, define $XY := \{xy : x \in X, y \in Y\}$.

Second isomorphism theorem.

If G is a group, $N \triangleleft G$ and $H \leq G$, then

1. $HN \leq G$,
2. $N \triangleleft HN$,
3. $H \cap N \triangleleft H$,
4. $HN/N \cong H/(H \cap N)$.

GROUP PRESENTATIONS.

The free group on generators x_1, \dots, x_n is the set of all words in the symbols $x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}$ equipped with concatenation, and is denoted $\langle x_1, \dots, x_n \rangle$.

Given an arbitrary group G , the normal closure $\text{ncl}_G(S)$ of a subset $S \subseteq G$ is the intersection of all normal subgroups of G which contain S ; that is, $\text{ncl}_G(S)$ is the ‘smallest’ normal subgroup of G which contains S . The group generated by x_1, \dots, x_n subject to ‘relations’ $r_1, \dots, r_k \in \langle x_1, \dots, x_n \rangle$ is

$$\langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle := \langle x_1, \dots, x_n \rangle / \text{ncl}_G(\{r_1, \dots, r_k\}).$$

If a group G is isomorphic to $\langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle$, then the latter is a ‘presentation’ of G . Also, $\langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle$ is equivalently the free group $\langle x_1, \dots, x_n \rangle$ subjected to the additional conditions $r_1 = \dots = r_k = e$ and all logical consequences thereof.

The n -th dihedral group D_n is the group of symmetries of a regular n -sided polygon; formally, D_n is defined for each $n \in \mathbb{Z}_{\geq 3}$ as the group generated by two elements, g and h , where g denotes reflection across a line through a specified, fixed vertex and h denotes rotation by $2\pi/n$ radians. There is a group presentation for D_n given by $D_n \cong \langle g, h \mid g^2, h^n, (gh)^2 \rangle$ for each $n \geq 3$.

Universal property of free groups.

Let G be a group generated by a set $\{s_1, \dots, s_n\}$ and $F = \langle S_1, \dots, S_n \rangle$ be the free group generated by the letters S_1, \dots, S_n . There exists a unique surjective group homomorphism $\pi : F \rightarrow G$ such that $\pi(S_i) = s_i$ for each $i \in \{1, \dots, n\}$.

FINITELY-GENERATED ABELIAN GROUPS.

In an abelian group, all subgroups are normal because left and right cosets must coincide; in a finite abelian group, all Sylow p -subgroups are unique. It follows that a finite abelian group is isomorphic to the direct product of its Sylow p -subgroups which implies:

Fundamental theorem of finite abelian groups.

1. A finite abelian group is isomorphic to a direct product of cyclic groups of prime power order uniquely up to reordering.

2. A finite abelian group of order n is isomorphic to a direct product of cyclic groups $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}$ where $n_i | n_{i+1}$ for all $1 \leq i \leq s-1$ and $n_1 n_2 \cdots n_s = n$ uniquely up to reordering the factors.

where the latter is implied by:

Chinese remainder theorem.

If $m, n \in \mathbb{Z} - \{0\}$ are coprime, then $C_{mn} \cong C_m \times C_n$.

Given a finite abelian group, the first and second decompositions are clearly isomorphic.

The exponent $e(G)$ of any finite group is the least common multiple of the orders of elements in G ; that is, the smallest n such that $g^n = e$ for all $g \in G$. Any finite abelian group G contains an element of order $e(G)$ so that if $e(G) = |G|$ then G is cyclic since such an element generates G .

The set of nonzero elements of a field form a group under multiplication in the field; that is, the *group of units* K^* of a field K given a field K . If A is a finite subgroup of K^* for a field K , then A is cyclic; as a consequence, the group of units of any finite field is cyclic.

If R is a ring, then an R -module is an abelian group $(M, +)$ equipped with a map $R \times M \rightarrow M$, $(r, m) \mapsto rm$ which is distributive, associative and unital. Given any ring R , the free R -module of rank s is the set of s -tuples R^s equipped with ‘pointwise’ addition and a map $R \times R^s \rightarrow R^s$ given by $r(r_1, \dots, r_s) \mapsto (rr_1, \dots, rr_s)$.

An abelian group G is a \mathbb{Z} -module equipped with the ‘obvious’ map $\mathbb{Z} \times G \rightarrow G$, $(n, a) \mapsto na$ where the latter is additive notation for $+$ in G . This observation leads to:

Fundamental theorem of finitely-generated abelian groups.

If A is a finitely-generated abelian group, then there exist $k, l \in \mathbb{N}$ and nonzero $r_1, \dots, r_k \in \mathbb{Z}$ with $r_i | r_{i+1}$ for each $1 \leq i \leq k-1$ such that $A \cong \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_k\mathbb{Z} \times \mathbb{Z}^l$ uniquely up to isomorphism.

whose proof is constructive as follows: given a \mathbb{Z} -module A finitely generated by s elements r_1, \dots, r_s , there exists an ‘obvious’ surjection $\varphi : \mathbb{Z}^s \rightarrow A$, $e_i \mapsto r_i$ for standard basis vectors e_i within \mathbb{Z}^s so that by the first isomorphism theorem for modules $\mathbb{Z}^s / \ker \varphi \cong \text{im } \varphi = A$; however, factor modules of \mathbb{Z}^s by a submodule such as $\ker \varphi$ are invariant up to isomorphism with respect to \mathbb{Z} -module automorphisms so as invertible row and column operations on the matrix ‘corresponding to’ a finitely generated submodule² are instances of such automorphisms, then $\mathbb{Z}^s / \ker \varphi$ is invariant under such operations upon the matrix ‘corresponding to’ $\ker \varphi$; we thereby build a matrix of the form $\text{diag}(r_1, \dots, r_k, 0, \dots, 0)$ which corresponds to a submodule of the form $K := \mathbb{Z}(r_1, 0, \dots, 0) + \cdots + \mathbb{Z}(0, \dots, 0, r_k, 0, \dots, 0)$ such that $A \cong \mathbb{Z}^s / K$ is exactly as desired where $l := s - k$ and we choose our operations so that $r_i | r_{i+1} \forall i$.

ALTERNATING GROUPS.

Given a set X , the set of bijections $X \rightarrow X$ forms a group under composition called the *symmetric group* $S(X)$ on X . The n -th finite symmetric group is $S_n := S(\{1, \dots, n\})$ so that for any finite set X of n elements, $S(X) \cong S_n$ via. the ‘obvious’ set bijection $\{1, \dots, n\} \rightarrow X$, with $|S_n| = n!$ for each n .

An element of S_n is often called a *permutation* and written either as an $2 \times n$ array or using cycle notation. Any permutation can be written uniquely (up to reordering) as a product of k disjoint cycles, or non-uniquely either as a product of transpositions (2-cycles) or adjacent transpositions (2-cycles of the form $(i \ i+1)$ for some i). The former implies for each $\sigma \in S_n$ a well-defined k -tuple called the *cycle type* of σ whose entries are the lengths of each disjoint cycle in decreasing order. A pair of permutations in S_n are conjugate iff they have the same cycle type; thus, conjugacy classes and cycle types in S_n are in exact one-to-one correspondence. Of explicit note also is that conjugation of a cycle (i_1, \dots, i_k) by an element $\tau \in S_n$ is given by $\tau(i_1 \cdots i_k)\tau^{-1} = (\tau(i_1) \cdots \tau(i_k))$ which generalises to any $\sigma \in S_n$ by writing $\sigma = c_1 c_2 \cdots c_k$ uniquely as disjoint cycles so that

$$\tau \sigma \tau^{-1} = \tau c_1 c_2 \cdots c_k \tau^{-1} = \tau c_1 (\tau^{-1} \tau) c_2 (\tau^{-1} \tau) \cdots (\tau^{-1} \tau) c_k \tau^{-1} = (\tau c_1 \tau^{-1}) (\tau c_2 \tau^{-1}) \cdots (\tau c_k \tau^{-1})$$

²i.e. given a submodule $K \subseteq \mathbb{Z}^s$ finitely generated by x_1, \dots, x_k , writing each $x_i = \sum_{j=1}^s a_{ij} e_j$ implies an $r \times s$ -matrix $(a_{ij}) \in \text{Mat}_{r \times s}(\mathbb{Z})$ associated to K so that $(a_{ij})(e_j) = (x_i)$.

via associativity in S_n .

Informally, the n -th alternating group A_n ‘is’ the subgroup of S_n consisting of even permutations, where an even/odd permutation is one which can be written as a product of an even/odd number of transpositions; for the latter to be formally well-defined, one approach constructs a group action of S_n a stabiliser of which is A_n .

Let x_1, \dots, x_n be indeterminates. Define $P := \prod_{1 \leq i < j \leq n} (x_i - x_j)$ so that S_n acts on $X := \{P, -P\}$ by permuting the indices. Observe that P consists of all possible distinct pairs $i < j$ within $\{1, \dots, n\}$; as each $\sigma \in S_n$ is a bijection, $\sigma.P = (-1)^k P$ where k is the number of pairs whose order σ ‘flips.’ A permutation $\sigma \in S_n$ is even if $\sigma.P = P$ and odd if $\sigma.P = -P$ and the n -th alternating group is the subset of S_n consisting of even permutations; immediately, $A_n = \text{Stab}_{S_n}(P) \leq S_n$.

The product of two even or two odd permutations is even, whereas that of an even and an odd permutation in either order is odd; thus, an n -cycle is even/odd iff n is odd/even. Moreover, $A_n \triangleleft S_n$ of index 2 so that $|A_n| = n!/2$ by Lagrange’s theorem.

Whereas $A_1, A_2 \cong 1$ and $A_3 \cong C_3$ are both simple, A_4 contains a unique non-trivial normal subgroup N of order 4 such that $A_4/N \cong C_3$ whereas $S_4/N \cong S_3$, meaning that A_4 is not simple. The observation that for any finite group G , a subgroup $N \leq G$ is normal iff it is a union of conjugacy classes (one of which is necessarily that of the identity) allows to prove by induction that A_n is simple for all $n \geq 5$ by exploiting five key facts:

1. $\text{Cl}_{A_n}(\sigma) \subseteq \text{Cl}_{S_n}(\sigma)$ for all $\sigma \in A_n$ (possibly a strict inclusion!),
 2. any pair of 3-cycles are conjugate in A_n for all $n \geq 5$ (i.e. equality holds in 1. for 3-cycles),
 3. A_n is generated by 3-cycles for all $n \geq 3$,
 4. for $H \leq S_n$ every non-trivial element of which is *fixed point free* (i.e. $\sigma(i) \neq i$ for all i), $|H| \leq n$.
 5. $|\text{Cl}_{A_n}(\sigma)| \geq n$ for all $n \geq 6$ and non-trivial $\sigma \in A_n$,
- and so conclude that A_n is not simple iff $n = 4$.

COMPOSITION SERIES AND THE JORDAN-HÖLDER THEOREM.

A composition series of a group G is a chain of normal subgroups

$$\{e\} =: G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{l-1} \triangleleft G_l := G \quad (*)$$

such that $G_i \neq G_{i-1}$ and G_{i-1}/G_i is simple for all $0 \leq i \leq l-1$. The observation that $\{e\} \triangleleft G$ is a composition series for G iff $G/\{e\} \cong G$ is simple implies a common analogy that composition series are to groups as prime factorisation is to the integers wherein simple groups are alike primes: those groups which cannot be ‘decomposed’ any further by means of a composition series.

The *composition factors* of the series are the factor groups G_{i+1}/G_i for all i and the *length* is the number of composition factors, in $(*)$ denoted l .

Jordan-Hölder theorem.

If G is a finite group, then there exists at least one composition series for G and any two composition series for G have the same length and composition factors up to isomorphism and reordering.

The Jordan-Hölder theorem states essentially that any finite group has one and ‘only’ one composition series; it does not however state that these uniquely *determine* a finite group. For instance, C_6 and S_3 both have composition series of length 2 and factors $\{C_2, C_3\}$, given by $\{e\} \triangleleft C_3 \triangleleft C_6$ and $\{e\} \triangleleft A_3 \triangleleft S_3$ respectively which are ‘the same’ in the Jordan-Hölder sense; only, C_6 and S_3 are not isomorphic since C_6 is abelian whereas S_3 is not abelian. Our simple group-prime number analogy here breaks down and also in that finite simple groups are entirely known as a result of the

Classification of finite simple groups.

If G is a finite simple group, then G is isomorphic to one of C_p for a prime p , A_n for $n \geq 5$, a group of Lie type³, or a sporadic group⁴.

³There are 16 infinite families together called groups of Lie type, such as the projective special linear groups over a finite field.

⁴These are 26 groups which don’t fit into any of the previous eighteen infinite families.

Proving Jordan-Hölder is informally summarised as follows: in both cases, we induct on $|G|$...

1. The base case $|G| = 1$ is trivial, as then $G = \{e\}$ which is a composition series (c.s.) for itself. Otherwise, let $|G| = k$ and suppose that any group with fewer than k elements has a composition series. If G is simple, then $\{e\} \triangleleft G$ is a c.s. for G as above; else, there exists a non-trivial $N \triangleleft G$. As $N \neq G$, then $|N| < k$ so N has a c.s.; as $N \neq \{e\}$, then $|N| > 1$ so by Lagrange's theorem $|G/N| < k$ so G/N also has a c.s. Using the canonical map $\text{can} : G \rightarrow G/N$ to pull back the latter to a chain of normal subgroups within G terminating at $N = \text{can}^{-1}(\{e_{G/N}\})$ and attaching this in the 'obvious' way to our c.s. for N yields a composition series for G .

2. The base case $|G| = 1$ is again trivial since $\{e\}$ has only one possible composition series, itself. Similarly, let $|G| = k$ and suppose that the latter part of the theorem holds for any group fewer than k elements. One takes a pair of arbitrary composition series for G and distinguishes between whether the penultimate elements of either chain are equal or distinct as normal subgroups of G , in the former case immediately using our assumption to obtain the result whereas in the latter case, one (more labouriously!) constructs four composition series for G which provide the result⁵.

SOLVABLE GROUPS.

A subnormal series for a group G is a chain of normal subgroups $\{e\} =: G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_l := G$. If $G_i \neq G_{i+1}$ for all $0 \leq i \leq l-1$, the chain is a series 'without repetition.' Every composition series is a subnormal series subject to the additional condition that each factor G_i/G_{i-1} is simple.

A group G is solvable if there exists a subnormal series for G such that each factor G_i/G_{i-1} is abelian. A group G is abelian iff it is solvable via. $\{e\} \triangleleft G$. This implies informally that a group is solvable if it can be decomposed into abelian groups via. a subnormal series.

Properties of solvable groups. If G is a finite abelian group of order $p_1^{n_1} \cdots p_k^{n_k}$, then the composition factors of G are C_{p_i}, \dots, C_{p_i} p_i -times for all $1 \leq i \leq k$ in some order; as a consequence, a finite group is solvable iff all composition factors are cyclic; for any group G and $N \triangleleft G$, it follows that G is solvable iff N and G/N are solvable.

If a group G is solvable and $H \leq G$, then H is solvable. For instance, A_n is solvable iff $n \leq 4$ meaning that S_n is not solvable for all $n \geq 5$. Any simple non-abelian group H is generally not solvable, since $\{e\} \triangleleft H$ is the only subnormal series of H and $H/\{e\} \cong H$ is not abelian.

Derived subgroups. The commutator of $a, b \in G$ is $[a, b] := aba^{-1}b^{-1}$ so that $[a, b] = e$ iff $ab = ba$ in G (i.e. a and b commute). The derived (or, commutator) subgroup is $G' := \langle [a, b] \mid a, b \in G \rangle$ so that $[a, b]^{-1} = [b, a]$ and $z[a, b]z^{-1} = [zaz^{-1}, zbz^{-1}]$ for all $z \in G$, meaning every element of G' is a product of commutators and thus $G' \triangleleft G$.

Since for all $N \triangleleft G$, G/N is abelian iff $G' \subseteq N$ and in particular taking $N = G'$ implies that G/G' is⁶ abelian, we interpret G' as the smallest normal subgroup N of G such that G/N is abelian.

Derived series. Iterating this construction implies that the *derived series* of a group G is the chain $G := G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots$ where $G^{(i+1)} = (G^{(i)})'$ for each i so that G is solvable iff there exists n for which $G^{(n)} = \{e\}$. Of note is that if there exists i such that $G^{(i+1)} = G^{(i)}$ then $G^{(j)} = G^{(i)}$ for all $j \geq i$ where if G is a finite group, such an i always exists: for instance, if G is simple and not abelian, then $G^{(i)} = G$ for all $i \geq 1$. The derived length of a solvable group G is the least n so that $G^{(n)} = \{e\}$. As an example, D_n has derived length 2 for all $n \geq 3$.

Feit-Thompson theorem.

If G is a finite group of odd order, then G is solvable.

⁵Each pair of c.s. for G correspond to c.s. one of the two distinct subgroups which allows us to similarly apply our assumption in either case.

⁶As G' is canonically defined for any group G , so too does the factor group G/G' always exist and is abelian, even if G itself is not abelian. It is therefore common to call G/G' the *abelianisation* of G , justified by the observation that $G/G' \cong G$ iff $G' = \{e\}$ iff G is abelian.