

PS6

Sasha Redden

March 10, 2026

1. For any group H , let H' be the **commutator** (or **derived**) subgroup which is the subgroup generated by all commutators $[g, h] = ghg^{-1}h^{-1}$. It is a normal subgroup and H/H' is abelian.

Let G be a finite group. The **derived series** is the sequence of subgroups defined recursively by $G^{(i+1)} = (G^{(i)})'$.

- (a) Find the derived series for D_n
 - (b) Assume that G is simple. Prove that $G' = G$ if and only if G is not abelian.
 - (c) Prove that G is solvable if and only if $G^{(n)} = \{1\}$ for some $n \geq 1$.
- (a) Since $srs^{-1} = r^{-1}$ is a relation in D_n for all n , we have that $[r, s] = rsr^{-1}s^{-1} = rrs = r^2$. Now we want to show that any commutator $[g, h]$ is in $\langle r^2 \rangle$.
 - i. Case 1. g, h are rotations, then they commute and $[g, h] = e$.
 - ii. Case 2. $g = r^k$ rotation and $h = r^m s$ reflection. Then $[g, h] = ghg^{-1}h = r^k r^m s r^{-k} r^m s = r^{k+m} s r^{m-k} s = r^{k+m} r^{-(m-k)} s s = r^{2k}$.
 - iii. Case 3. $g = r^m s$ reflection and $h = r^k$ rotation. Since $(ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1}$, from above, $[g, h] = r^{-(2k)} = (r^{-k})^2$.
 - iv. Case 4. $g = r^k s, h = r^m s$ both reflections, then $[g, h] = (gh)^2 = (r^k s r^m s)^2 = (r^{k-m} s s)^2 = (r^{k-m})^2$.

Thus $D'_n = \langle r^2 \rangle$ and since if n is odd $\langle r^2 \rangle = \langle r \rangle \cong \mathbb{Z}/n$, otherwise $n = 2m$ and $\langle r^2 \rangle \cong \mathbb{Z}/m$, so either way $\langle r^2 \rangle$ is abelian so the commutator subgroup $\langle r^2 \rangle' = \{e\}$ so the commutator subgroup for D_n is:

$$\{1\} \leq \langle r^2 \rangle \leq D_n$$

- (b) Assume $G' = G$, suppose G is abelian, but then $G' = \{e\}$, so G is not abelian. Now assume G is not abelian, since G is simple, G' must be either G or $\{e\}$, but G is not abelian so $G' = G$.
- (c) Assume G is solvable, then there exists a tower of subgroups $\{1\} = G_m \leq G_{m-1} \leq \dots \leq G_0 = G$ where $G_{i+1} \triangleleft G_i$ and G_i/G_{i+1} is cyclic (or abelian?), since the commutator G'

is the smallest normal subgroup such that G/G' is abelian, then $G' \subseteq G_1$, and it follows that $G^{(i)} \subseteq G_i$ for all i , then we must have $G_m = G^{(m)} = \{1\}$.

2. Let G be a finite group. Let $Z_1 = Z(G)$, the centre of G . For $i = 1, \dots$ let

$$Z_{i+1} = \{g \in G : \forall h \in G, [g, h] \in Z_i\}$$

This is called the **upper central series**:

$$Z_0 = \{1\} \leq Z_1 \leq Z_2 \leq \dots$$

G is called **nilpotent** if there exists n such that $Z_n = G$.

- (a) Prove that each Z_i is normal in G .
- (b) Prove that if G is nilpotent then it is solvable.
- (c) Prove that all p -groups are nilpotent (groups whose order is the power of a prime.)
- (d) Find a solvable group that is not nilpotent.

- (a) **Proof by induction:**

Base case: $i = 1$, $Z_1 = Z(G) = \{z \in G : \forall g \in G, zg = gz\}$, then $\forall z \in Z(G)$, $\forall g \in G, gzg = z \in Z(G)$ so $Z(G)$ is normal.

Inductive hypothesis: Assume Z_k is normal in G for all $k < i$, want to show Z_{k+1} is normal in G .

Let $g \in Z_{k+1}$, then $\forall h_1 \in G, [g, h_1] = gh_1g^{-1}h_1^{-1} \in Z_k$. We want to show that $\forall h_2 \in G, h_2gh_2^{-1} \in Z_{k+1}$ i.e. $\forall h_1 \in G, [h_2gh_2^{-1}, h_1] \in Z_k$.

$$[h_2gh_2^{-1}, h_1] = h_2gh_2^{-1}h_1(h_2gh_2^{-1})^{-1}h_1^{-1} = h_2gh_2^{-1}h_1h_2g^{-1}h_2^{-1}h_1^{-1} = h_2gh_2^{-1}(h_1h_2)g(h_1h_2)^{-1}$$

Then multiplying by $1 = g^{-1}g$ after $h_2gh_2^{-1}$ we obtain

$$(h_2gh_2^{-1}g^{-1})(g(h_1h_2)g^{-1}(h_1h_2)^{-1}) = [h_2, g][g, h_1h_2] = [g, h_2]^{-1}[g, h_1h_2]$$

Since $g \in Z_{k+1}$, $[g, h_2]$ and $[g, h_1h_2] \in Z_k$, then $[h_2gh_2^{-1}, h_1] \in Z_k$ so $h_2gh_2^{-1} \in Z_{k+1}$ and thus Z_{k+1} is normal in G .

- (b) Suppose there exists n such that $Z_n = G$, then there is series of (normal) subgroups:

$$\{1\} = Z_0 \leq Z_1 \leq \dots \leq Z_n = G$$

Where $Z_i \triangleleft Z_{i+1}$ and by transitivity of normal subgroups, $Z_i \triangleleft G \forall i$. Since Z_{i+1}/Z_i is central in G/Z_i , $Z_{i+1}/Z_i = Z(G/Z_i)$, so Z_{i+1}/Z_i is abelian and G is solvable.

- (c) Let G be a p -group such that $|G| = p^n$ for some n . We know that G has a non-trivial center. Suppose $Z(G) \neq G$ i.e. G is not abelian, because otherwise we are done. Then there exists $g \in G \setminus Z(G)$ such that there exists i where $g \in Z_i$, because G/Z_i is a p -group as well, so it has a non-trivial center $Z(G/Z_i) = Z_{i+1}/Z_i$.
- (d) S_3 is not nilpotent because $Z(S_3) = \{1\}$ and solvable because $S_3 \cong D_3$ with derived series $\{1\} \leq \langle r^2 \rangle \leq D_3$.

3. It is known that every non-abelian finite simple group has even order. Use this fact to prove that every group of odd order is solvable. (This is called the Feit-Thompson theorem.)

Using the contrapositive of the statement, if the order of G is odd, then G is not non-abelian and simple, so G is abelian and simple, abelian and non-simple, or non-abelian and non-simple. If G is abelian then it is solvable by 1.c because the commutator subgroup $G' = \{1\}$. Now suppose G is non-abelian and non-simple, then there exists a non-trivial commutator subgroup G' , if G' is also non-simple then again there is a non-trivial commutator subgroup. Eventually there will be an abelian $G^{(i)}$ because G is finite so there must be an i such that $G^{(i)}$ is simple, and if $G^{(i)}$ is simple and non-abelian, then by the above fact, it must have even order, but this is a contradiction because $|G|$ is odd so it does not have any even order subgroups, so $G^{(i)}$ must be abelian. Then again we have that either $G^{(i)} = \{1\}$ or $G^{(i+1)} = \{1\}$, in either case there is an $n \geq 1$ such that $G^{(n)} = \{1\}$ and so by 1.c G is solvable. $\square$

4. Let $a \in \mathbb{F}_p$, and assume $a \neq 0$. Let F be the splitting field of $x^p - x - a$ over $\mathbb{F}_p$.

- (a) Prove that $x^p - x - a$ is irreducible.
- (b) Prove that if $f(c) = 0$ then $f(c + 1) = 0$
- (c) Prove that $[F : \mathbb{F}_p] = p$.
- (d) Show that $\text{Gal}(F/\mathbb{F}_p) \cong \mathbb{Z}/p$.

- (a) By Fermat's little theorem, for any prime p , $a^p \equiv a \pmod{p}$, then for any $x \in \mathbb{F}_p$, $x^p = x$, so $f(x) = x^p - x - a = x - x - a = -a \neq 0$, then $f(x)$ is constant in $\mathbb{F}_p$ so it is irreducible.

- (b) Suppose $f(c) = 0$ for some c . $f(x + 1) = (x + 1)^p - (x + 1) - a$ and

$$(x + 1)^p = \sum_{k=0}^p \binom{p}{k} x^k = 1 + \binom{p}{1} x + \binom{p}{2} x^2 + \cdots + \binom{p}{p-1} x^{p-1} + x^p \equiv 1 + x^p \pmod{p}$$

because $p \mid \binom{p}{k}$ for $k = 1, \dots, p-1$. So $f(c + 1) = 1 + c^p - c - 1 - a = c^p - c - a = 0$.

- (c) Let α be a root of $f(x)$, then from b, by induction, $\alpha + 1, \alpha + 2, \dots$ are all roots of $f(x)$, but $\alpha + p \equiv \alpha \pmod{p}$, so there are exactly p distinct roots of $f(x)$, thus $F = \mathbb{F}_p(\alpha, \alpha + 1, \dots, \alpha + p - 1)$ so $[F : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(F) = p$.

- (d) Since F is the splitting field of a separable polynomial in $\mathbb{F}_p$, $F/\mathbb{F}_p$ is a Galois extension and thus $|\text{Gal}(F/\mathbb{F}_p)| = p$. Let $k \in \mathbb{Z}/p$, then there exists a unique $\sigma_k \in \text{Gal}(F/\mathbb{F}_p)$ such that $\sigma_k(\alpha) = \alpha + k \pmod{p}$ for root α of $f(x)$ and $\sigma_k(q) = q \ \forall q \in \mathbb{F}_p$, and since there are p of these automorphisms, $\text{Gal}(F/\mathbb{F}_p) = \{\sigma_k : k \in \mathbb{Z}/p\}$.

Claim: There is an isomorphism $\varphi : \text{Gal}(F/\mathbb{F}_p) \rightarrow \mathbb{Z}/p$ such that $\varphi(\sigma_k) = k$ for all $k \in \mathbb{Z}/p$.

Proof: Let $n, k \in \mathbb{Z}/p$, then for any $q \in \mathbb{F}_p$, $\sigma_n \circ \sigma_k(q) = q = \sigma_{n+k}(q)$ and for $\alpha \in F \setminus \mathbb{F}_p$, $\sigma_n \circ \sigma_k(\alpha) = \sigma_n(\sigma_k(\alpha)) = \sigma_n(\alpha + k) = \alpha + k + n = \sigma_{n+k}(\alpha)$. Then

$$\varphi(\sigma_n \circ \sigma_k) = \varphi(\sigma_{n+k}) = n + k = \varphi(\sigma_n) + \varphi(\sigma_k)$$

and since $|\text{Gal}(F/\mathbb{F}_p)| = p = \mathbb{Z}/p$, and this map is injective because if $\varphi(\sigma_n) = m = \varphi(\sigma_k)$ then $n = m = k$, so φ is an isomorphism, thus $\text{Gal}(F/\mathbb{F}_p) \cong \mathbb{Z}/p$. $\square$
 realized after I wrote this that you can just stop at $|\text{Gal}(F/\mathbb{F}_p)| = p$ because $\mathbb{Z}/p$ is the only group of size p oops!!