§ 6 Commutators and the derived series

Definition. Let G be a group, and let $x, y \in G$. The *commutator* of x and y is

$$[x,y] = xyx^{-1}y^{-1}.$$

Note that $[x,y] = e$ if and only if $xy = yx$ (since $x^{-1}y^{-1} = (yx)^{-1}$).

Proposition 33. *Let G be a group, and let $N \trianglelefteq G$. Then G/N is abelian if and only if $[x,y] \in N$ for all $x, y \in G$.*

Proof. Suppose $[x,y] \notin N$. Then in G/N we have

$$[xN, yN] = xNyNx^{-1}Ny^{-1}N = [x,y]N \neq N.$$

So $[xN, yN] \neq e_{G/N}$, and so xN and yN do not commute. Conversely, if $[x,y] \in N$ for all x, y, then $[xN, yN] = e_{G/N}$ for all $x, y \in G$, and so G/N is abelian. □

Definition. Let G be a group, and let $X, Y \leq G$. We write $[X,Y]$ for the subgroup of G generated by the commutators $\{[x,y] \mid x \in X, y \in Y\}$. We write G' for $[G,G]$, the *derived subgroup* or *commutator subgroup* of G.

Remarks.

1. **Important!** The product of two commutators need not itself be a commutator, and so the set of all commutators in G is not necessarily a subgroup. To put this another way, the derived group G' may contain elements which are not commutators.
2. The inverse of the commutator $[x,y]$ is a commutator, namely $[y,x]$. So if $X, Y \leq G$ then $[X,Y] = [Y,X]$.
3. If $X \trianglelefteq G$ and $Y \leq G$, then $[X,Y] \leq X$, since $xyx^{-1}y^{-1} = x\,{}^{y}x^{-1}$.

Proposition 34. *Let G be a group. If $X, Y \trianglelefteq G$ then $[X,Y] \trianglelefteq G$. In particular, $G' \trianglelefteq G$.*

Proof. Let $g \in G$, and let $x \in X$, $y \in Y$. Then

$${}^{g}[x,y] = {}^{g}(xyx^{-1}y^{-1}) = {}^{g}x\,{}^{g}y\,{}^{g}x^{-1}\,{}^{g}y^{-1} = [{}^{g}x, {}^{g}y].$$

Since X and Y are normal, ${}^{g}x \in X$ and ${}^{g}y \in Y$, and so ${}^{g}[x,y] \in [X,Y]$.

Now suppose that $z \in [X,Y]$. Then

$$z = [x_1, y_1][x_2, y_2] \cdots [x_k, y_k],$$

for some $x_1, \ldots, x_k \in X$ and $y_1, \ldots, y_k \in Y$. Now

$${}^{g}z = {}^{g}[x_1, y_1] \cdots {}^{g}[x_k, y_k] \in [X,Y],$$

as required. □

Remark. By Proposition 33, we see that G' is the unique smallest normal subgroup of G such that G/G' is abelian. (For $N \trianglelefteq G$, we have that G/N is abelian if and only if $G' \leq N$.) The quotient G/G' is called the *abelianization* of G, written G^{ab}.

Definition. A subgroup H of G is *characteristic* if $\varphi(H) = H$ for every $\varphi \in \text{Aut}(G)$. We write $A \operatorname{char} G$.

This is a strengthening of the condition for normality. To be a normal subgroup, H has only to be invariant under the *inner* automorphisms.

Proposition 35. *If* $A, B \operatorname{char} G$ *then* $[A,B] \operatorname{char} G$.

Proof. Same as Proposition 34. □

Proposition 36. *Let* G *be a group.*

1. *If* $N \trianglelefteq G$ *and* $X \operatorname{char} N$*, then* $X \trianglelefteq G$.

2. *If* $N \operatorname{char} G$ *and* $X \operatorname{char} N$ *then* $X \operatorname{char} G$.

Proof. If $\alpha(N) = N$, then the restriction $\alpha|_N$ of α to N is an automorphism of N. So if $X \operatorname{char} N$, then $\alpha(X) = \alpha|_N(X) = X$. It follows that if $N \trianglelefteq G$, then X is invariant under all inner automorphisms of G, and so $X \trianglelefteq G$. If $N \operatorname{char} G$ then X is invariant under all automorphisms of G, and so $X \operatorname{char} G$. □

Warning. It is possible that $N \operatorname{char} G$ and $X \trianglelefteq N$, but $X \ntrianglelefteq G$. An example is $G = S_4$, $N = V_4$, and $X = \langle (1\,2)(3\,4) \rangle$.

Definition. The *derived series* of a group G is the series of subgroups

$$G^{(0)} \geq G^{(1)} \geq \cdots$$

defined by

$$G^{(0)} = G,$$
$$G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

Proposition 37. $G^{(i)} \operatorname{char} G$ *for all* i.

Proof. We use induction. Certainly $G^{(0)} = G \operatorname{char} G$. Suppose that $G^{(i)} \operatorname{char} G$. Since $G^{(i+1)}$ is the derived subgroup of $G^{(i)}$, we have $G^{(i+1)} \operatorname{char} G^{(i)}$ by Proposition 35. So $G^{(i+1)} \operatorname{char} G$ by Proposition 36.2. □

Examples.

1. Let A be abelian. Then $[a,b] = e$ for all $a, b \in A$, and so the derived series of A is

$$A \geq \{e\} \geq \{e\} \geq \cdots .$$

2. Let $G = D_{2n}$, and let C_n be the rotation subgroup of G. For d dividing n, let C_d be the unique subgroup of C_n of order d.
Let $x \in G$ be a generator of C_n. Since G/C_n has order 2, it is abelian, and so we have $G' \le C_n$. Let y be a reflection. Then $[x,y] = xyx^{-1}y^{-1} = x^2$. It follows that $\langle x^2 \rangle \le G'$. So G' is either equal to C_n or to $\langle x^2 \rangle$.
If n is odd, then $\langle x^2 \rangle = C_n$, and so the derived series for D_{2n} in this case is

$$D_{2n} \ge C_n \ge \{e\} \ge \cdots .$$

If n is even then $\langle x^2 \rangle = C_{n/2}$. Now $G/C_{n/2}$ has order 4, and so it is abelian. Hence $G' \le C_{n/2}$, and it follows that $G' = C_{n/2}$. The derived series for D_{2n} in this case is

$$D_{2n} \ge C_{n/2} \ge \{e\} \ge \cdots .$$

3. Since S_4/A_4 is abelian, we have $S_4' \le A_4$. But $S_4/V_4 \cong S_3$ is not abelian, and so $S_4' \not\le V_4$. So S_4' is a normal subgroup of S_4 contained in A_4 but not V_4, and therefore we have $S_4' = A_4$.
Similarly, we see that A_4/V_4 is abelian, but $A_4/\{e\}$ is not. So A_4' is a normal subgroup of A_4 contained in V_4 but not $\{e\}$, and hence $A_4' = V_4$.
So the derived series of S_4 is

$$S_4 \ge A_4 \ge V_4 \ge \{e\} \ge \cdots .$$

4. The normal subgroups of S_5 are S_5, A_5 and $\{e\}$. The smallest normal subgroup giving an abelian quotient group is A_5. So $S_5' = A_5$. Now A_5 is simple, and so A_5' is $\{e\}$ or A_5. Since $A_5/\{e\}$ is not abelian, we have $A_5' = A_5$. So the derived series of S_5 is

$$S_5 \ge A_5 \ge A_5 \ge \cdots .$$

The derived series of S_n for $n > 5$ is similar.

Proposition 38. *Let G be a finite group. Then G is soluble if and only if $\{e\}$ appears in the derived series of G.*

Proof. Since G is finite, there exists some i such that $G^{(i)} = G^{(i+1)}$. Clearly we now have $G^{(k)} = G^{(i)}$ for all $k \ge i$, and so $\{e\}$ appears in the derived series if and only if $G^{(i)} = \{e\}$. Suppose that $G^{(i)} \ne \{e\}$. Let

$$G^{(i)} = H_0 > H_1 > \cdots > H_k = \{e\}$$

be a composition series for $G^{(i)}$. Since $G^{(i+1)} \not\le H_1$, and since $G^{(i+1)}$ is the derived subgroup of $G^{(i)}$, it follows that H_0/H_1 is non-abelian. So $G^{(i)}$ is not soluble. Now we see that G is not soluble, by Proposition 32.

Now suppose that $G^{(i)} = \{e\}$. By repeated application of Proposition 28.2, there exists a composition series for G which includes $G^{(j)}$ for all $j \le i$. But now it is clear that all of the composition factors are abelian, since $G^{(j)}/G^{(j+1)}$ is abelian for all j. So G is soluble. □

Remark. Proposition 38 suggests a way of defining solubility for infinite groups. For an arbitrary G, we say that G is soluble if $G^{(i)} = \{e\}$ for some $i \in \mathbb{N}$. This agrees with our earlier definition when G is finite.

§ 7 The lower central series and nilpotent groups

Definition. Let G be a group. The *lower central series* of G is the series

$$\gamma_1(G) \geq \gamma_2(G) \geq \cdots$$

defined by

$$\gamma_1(G) = G,$$
$$\gamma_{i+1}(G) = [\gamma_i(G), G].$$

Remark. Comparing the definitions of the derived series and the lower central series, it is clear that $\gamma_1(G) = G^{(0)} = G$ and $\gamma_2(G) = G^{(1)} = G'$. Beyond this the series are not generally equal. In the proof of Proposition 39 below we shall show that $\gamma_{i+1}(G) \geq G^{(i)}$ for all i.

Warning. Note that the lower central series conventionally starts with γ_1, not γ_0. (There is a good reason for this; see Theorem 43 below.)

Examples.
1. If A is abelian, then $\gamma_1(A) = A$, and $\gamma_i(A) = \{e\}$ for $i \geq 2$.
2. Let $G = D_{2n}$, and let C_d be the rotation subgroup of order d, for d dividing n. We have seen that

$$\gamma_2(G) = G' = \begin{cases} C_n & \text{if } n \text{ is odd,} \\ C_{n/2} & \text{if } n \text{ is even.} \end{cases}$$

Now let x be any rotation in G, and let $g \in G$. We have

$$[a, g] = \begin{cases} e & \text{if } g \text{ is a rotation,} \\ a^2 & \text{if } g \text{ is a reflection.} \end{cases}$$

It follows that

$$[C_d, G] = \begin{cases} C_d & \text{if } d \text{ is odd,} \\ C_{d/2} & \text{if } d \text{ is even.} \end{cases}$$

This allows us to write down the lower central series for D_{2n} easily. For instance, the lower central series for D_{16} and D_{24} are

$$D_{16} > C_4 > C_2 > \{e\} > \cdots,$$

$$D_{24} > C_6 > C_3 > C_3 > \cdots.$$

Definition. A group G is *nilpotent* if its lower central series includes $\{e\}$. If $\gamma_{c+1}(G) = \{e\}$, and if c is the smallest number for which this is the case, then G has *nilpotency class* c.

So D_{16} is nilpotent of class 3, while D_{24} is not nilpotent. The trivial group is the unique group with nilpotency class 0; a group has nilpotency class 1 if and only if it is a non-trivial abelian group.

Proposition 39. *Any nilpotent group is soluble.*

Proof. We first that $G^{(i)} \leq \gamma_{i+1}(G)$ for all $i \geq 0$. This is certainly the case for $i = 0$, since $G^{(0)} = \gamma_1(G) = G$. Suppose that $G^{(i)} \leq \gamma_{i+1}(G)$ for some i. Then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [\gamma_{i+1}(G), G] = \gamma_{i+2}(G),$$

as required. (Here we have used the obvious fact that if $A \leq C$ and $B \leq D$ then $[A,B] \leq [C,D]$.)

Now if G is nilpotent, then $\gamma_{c+1}(G) = \{e\}$ for some c. But then $G^{(c)} = \{e\}$, and so G is soluble. □

Remark. We have seen that D_{24} is soluble but not nilpotent. So nilpotency is a stronger condition than solubility.

Proposition 40. *Let $N \trianglelefteq G$. Then $[N,G]$ is the smallest normal subgroup of G contained in N, such that N/K is central in G/K. (That is, N/K is contained in the centre of G/K.)*

Proof. We certainly have that $[N,G]$ is a normal subgroup of G, by Proposition 34, and it is contained in N since N is normal. Let $K \trianglelefteq G$, with $K \leq N$. For $x \in N$ we have

$$xK \in Z(G/K) \Longleftrightarrow xKgK = gKxK \Longleftrightarrow [x,g] \in K \text{ for all } g \in G,$$

and so xK is central in G/K if and only if $[N,G] \leq K$. □

Corollary 41. *$\gamma_i(G)/\gamma_{i+1}(G)$ is central in $G/\gamma_{i+1}(G)$ for all i.*

Examples.

1. We already know $\gamma_1(S_4) = S_4$ and $\gamma_2(S_4) = A_4$, since the lower central series agrees with the derived series in its first two terms. Now $\gamma_3(S_4)$ is a subgroup K, normal in S_4 and contained in A_4, and such that A_4/K is central in S_4/K. But of the normal subgroups of S_4, we see that $A_4/\{e\}$ is not central in $S_4/\{e\}$ and A_4/V_4 is not central in S_4/V_4. So we have $\gamma_3(S_4) = A_4$. So the lower central series of S_4 is

$$S_4 \geq A_4 \geq A_4 \geq \cdots .$$

2. We have $\gamma_1(A_4) = A_4$, and $\gamma_2(A_4) = [A_4, A_4] = V_4$. Now $\gamma_3(A_4)$ is a normal subgroup of A_4 contained in V_4, and so it is either $\{e\}$ or V_4. But $V_4/\{e\}$ is not central in $A_4/\{e\}$. So $\gamma_3(A_4) = V_4$, and the lower central series for A_4 is

$$A_4 \geq V_4 \geq V_4 \geq \cdots .$$

Remark. If H is in the derived series for G, then the series for G below H is the same as the derived series for H. This is not true for the lower central series (see the case of S_4 and A_4 above). Unlike the derived series, the recursion which defines successive terms of the lower central series involves the starting point for the series, as well as the current term.

Proposition 42. *$\gamma_i(G)$ char G for all i.*

Proof. This is an easy induction, using Proposition 35. □

Theorem 43
For any $i, j \in \mathbb{N}$, we have

$$[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G).$$

The proof of Theorem 43 is a little intricate, and relies on two preliminary lemmas.

Lemma 44 (Witt's Lemma)**.** *Let G be a group, and let $a, b, c \in G$. Then*

$$^{a}[[a^{-1}, b], c]\, ^{c}[[c^{-1}, a], b]\, ^{b}[[b^{-1}, c], a] = e.$$

Proof. Multiplying out the left-hand side, we get

$$(aa^{-1}bab^{-1}cba^{-1}b^{-1}ac^{-1}a^{-1})\,(cc^{-1}aca^{-1}bac^{-1}a^{-1}cb^{-1}c^{-1})\,(bb^{-1}cbc^{-1}acb^{-1}c^{-1}ba^{-1}b^{-1}),$$

in which all the terms cancel. □

Lemma 45 (Three subgroup lemma)**.** *Let G be a group, and let A, B, C be subgroups. Let $N \trianglelefteq G$. If $[[A,B],C] \leq N$ and $[[C,A],B] \leq N$, then $[[B,C],A] \leq N$.*

Proof. By definition, $[[B,C],A]$ is generated by the elements $[x,a]$ with $x \in [B,C]$ and $a \in A$. Any element $x \in [B,C]$ is a product of commutators $[b,c]$ with $b \in B$ and $c \in C$. Now we observe that the identity

$$[xy, a] = {}^{x}[y,a] \cdot [x,a]$$

holds for all $x, y, a \in G$; this is easily verified by writing out the commutators explicitly. It follows that $[[B,C],A]$ can be generated by elements of the form $^{z}[[b,c],a]$, where $a \in A$, $b \in B$, $c \in C$ and $z \in [B,C]$.

Take an arbitrary commutator $[b^{-1},c],a] \in [[B,C],A]$. Then

$$\left(^{b}[[b^{-1}, c], a]\right)^{-1} = {}^{a}[[a^{-1}, b], c]\, ^{c}[[c^{-1}, a], b],$$

by Witt's Lemma. Now $[[a^{-1},b],c] \in [[A,B],C] \leq N$, and since N is normal, we have $^{a}[[a^{-1},b],c] \in N$. Similarly $^{c}[[c^{-1},a],b] \in N$, and so $^{b}[[b^{-1},c],a] \in N$. But N is normal, and so $^{z}[[b^{-1},c],a] \in N$ for all $z \in G$ (and in particular, for all $z \in [B,C]$.

Since the elements ${}^{z}[[b^{-1},c],a]$ generate $[[B,C],A]$, we have $[[B,C],A] \leq N$. □

Proof of Theorem 43. We work by induction on j, the inductive hypothesis being

$$\mathbb{P}(j)\colon \text{ for all } i,\ [\gamma_i(G),\gamma_j(G)] \leq \gamma_{i+j}(G).$$

We see that $\mathbb{P}(1)$ is true, since

$$[\gamma_i(G),\gamma_1(G)] = [\gamma_i(G),G] = \gamma_{i+1}(G).$$

Suppose inductively that $\mathbb{P}(j)$ is true. Consider the three subgroup lemma with

$$A = \gamma_i(G), \quad B = \gamma_j(G), \quad C = G, \quad N = \gamma_{i+j+1}(G).$$

Invoking $\mathbb{P}(j)$, we see that

$$[[A,B],C] = [[\gamma_i,\gamma_j],G] \leq [\gamma_{i+j}(G),G] = \gamma_{i+j+1}(G) = N,$$

$$[[C,A],B] = [[G,\gamma_i(G)],\gamma_j(G)] = [\gamma_{i+1}(G),\gamma_j(G)] = [\gamma_j(G),\gamma_{i+1}(G)] \leq \gamma_{i+j+1}(G) = N.$$

So the conditions of the Three subgroup lemma are fulfilled, and thus we have $[[B,C],A] \in N$. Hence for all i we have

$$[\gamma_{j+1}(G),\gamma_i(G)] = [[\gamma_j(G),G],\gamma_i(G)] \leq \gamma_{i+j+1}(G),$$

which establishes $\mathbb{P}_{j+1}$. □

Definition. Let G be a group. A series of subgroups

$$G = G_0 > G_1 > \cdots > G_k = \{e\}$$

such that G_i/G_{i+1} is central in G/G_{i+1} for all i is called a *central series* for G. The *length* of the central series is k.

Warning. The lower central series is only a central series when G is nilpotent. (This, unfortunately, is standard terminology.)

Proposition 46. *Let G be a group, and let $\{G_i\}$ be a central series for G. Then $\gamma_{i+1}(G) \leq G_i$ for all i.*

Proof. We use induction on i. Certainly we have $\gamma_1(G) = G = G_0$. Suppose that $\gamma_{i+1}(G) \leq G_i$ for some i. Then

$$\gamma_{i+2}(G) = [\gamma_{i+1}(G),G] \leq [G_i,G].$$

But $[G_i,G] \leq G_{i+1}$ by Proposition 40, since $G_i/G_{i+1} \in Z(G/G_{i+1})$. □

Corollary 47. *If G has a central series, then G is nilpotent.*

Proof. Let $\{G_i\}$ be a central series of length k. Then $\gamma_{k+1}(G) \leq G_k = \{e\}$, and so $\gamma_{k+1}(G) = \{e\}$. So G is nilpotent. □

Definition. Let G be a group. The *upper central series* for G is the series

$$\{e\} = Z_0(G) \leq Z_1(G) \leq \cdots ,$$

defined by

$$Z_0(G) = \{e\},$$
$$\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right).$$

Note that in the correspondence given by Proposition 2, Z_{i+1} is the subgroup of G corresponding to the centre of $G/Z_i(G)$, and so this definition makes sense.

Remark. Since $Z_1(G)/\{e\} = Z(G/\{e\})$, it is clear that $Z_1(G) = Z(G)$. The subgroup $Z_i(G)$ is sometimes called the i-th centre of G.

Warning. The upper central series is a central series (in reverse) only if $Z_k(G) = G$ for some $k \in \mathbb{N}$. As we shall see, this is the case if and only if G is nilpotent.

Proposition 48. *Let G be a group, and let $\{G_i\}$ be a central series for G of length k. Then $G_{k-i} \leq Z_i(G)$ for $0 \leq i \leq k$.*

Proof. We work by induction on i. Certainly we have $G_{k-0} = \{e\} = Z_0(G)$. Suppose that $G_{k-i} \leq Z_i(G)$ for some i. Since

$$\frac{G_{k-i-1}}{G_{k-i}} \leq Z\left(\frac{G}{G_{k-i}}\right),$$

we have $[G_{k-i-1}, G] \leq G_{k-i}$ by Proposition 40. So $[G_{k-i-1}, G] \leq Z_i(G)$, and so

$$\frac{G_{k-i-1}}{Z_i(G)} \leq Z\left(\frac{G}{Z_i(G)}\right),$$

by Proposition 40 again. So $G_{k-i-1} \leq Z_{i+1}(G)$. □