11. SOLUBLE GROUPS

§ 11.1. The Derived Series

Recall that the derived (commutators) subgroup is generated by all the commutators 
\[ [a, b] = a^{-1}b^{-1}ab \] for all \( a, b \). The derived subgroup of \( G \) is denoted by \( G' \) and it is the largest normal subgroup for which the quotient group is abelian. This is usually the quickest way of finding it. We can continue the process, giving a whole series of subgroups.

We define \( G'' = (G')' \) and \( G''' = (G'')' \) etc. We denote the \( n \)-th derived subgroup (the result of \( n \) such steps) by \( G^{(n)} \) so \( G''' = G^{(3)} \). In other words we define \( G^{(n)} \) inductively by: 
\[ G^{(0)} = G; \quad G^{(n+1)} = G^{(n)}' \]

This results in a chain of subgroups: 
\[ G \geq G' \geq G'' \geq G''' \geq ... \]
Each subgroup is normal in the one before and the quotients of successive terms are abelian. Such a series is called the derived series for \( G \).

Example 1: \( S_4' = A_4, S_4'' = V_4 \) and \( S_4''' = S_4^{(3)} = 1 \).
Here \( V_4 = \{1, (12)(34), (13), (24), (14)(23)\} \) is the normal subgroup of order 4. Because \( A_4/V_4 \) has order 12/4 = 3, it is cyclic, and hence abelian, so \( S_4'' = A_4' \leq V_4 \). Thus \( S_4'' \) has order 1, 2 or 4. It’s not 1 because \( A_4 \) is not abelian. It’s not of order 2 because then \( A_4/A_4' \) would have to be cyclic of order 6, yet \( A_4 \) has no elements of order 6.
This leaves \( S_4'' = A_4' = V_4 \). Finally, since \( V_4 \) is abelian \( S_4''' = V_4' = 1 \).

In a case like this, where the derived series of a group \( G \) reaches the “bottom”, we say that \( G \) is a soluble group. More precisely, we say that \( G \) is soluble of length \( n \) if \( n \) is the smallest integer such that \( G^{(n)} = 1 \). Non-trivial abelian groups are thus soluble of length 1, dihedral groups whose order is at least 6 are soluble of length 2. \( S_4 \) is the smallest soluble group of length 3 and \( GL(2,3) \) has soluble length 4.

Theorem 1: Subgroups and quotient groups of soluble groups are soluble.
Proof: If \( H \leq G \) then \( H' \leq G' \) and so inductively \( H^{(n)} \leq G^{(n)} \) for all \( n \).

By the first isomorphism a quotient group \( G/K \) is isomorphic to the image, \( H \), of some homomorphism \( f \) from \( G \) onto \( H \), with kernel \( K \). Clearly \( f(G') = H' \), because the image of a commutator is a commutator. More generally \( f(G^{(n)}) = H^{(n)} \). So if \( G \) is soluble then \( G^{(n)} \) is trivial for some \( n \) and so \( H^{(n)} \) must therefore be trivial.

The soluble length of a subgroup or quotient group cannot exceed that of the group itself, but it may be less.

There are two ways that a group can fail to be soluble. The derived series might continue to descend indefinitely.
\[ G > G' > G'' > G''' > G^{(4)} > ... \]
Of course this can only occur for an infinite group. But a group, even a finite one, can fail to be soluble by virtue of its derived series getting “stuck” at some point, that is, where it reaches a subgroup that is not the identity but which, like the identity subgroup, is equal to its...
own derived subgroup. One very special way this can happen is for a non-abelian group to have no normal subgroups other than itself and the identity.

§ 11.2. Simple Groups

A group $G$ that has no normal subgroups, apart from $G$ itself and 1, is called a simple group. Such groups are “simple” so far as their lattice of normal subgroups goes. But in other respects most of them are far from “simple”, in the normal sense of the word. But let’s get the really “simple” simple groups out of the way.

Groups of prime order (necessarily cyclic) are simple groups. This is a direct consequence of Lagrange’s Theorem. These groups, together with the trivial group 1, are in fact the only abelian simple groups. (Why?).

So the only simple groups of real interest are the non-abelian ones. Among these the finite non-abelian simple groups have attracted an enormous amount of interest over the last hundred years. A classification of the finite simple groups has now been finished. But it was an enormous task.

The Guinness Book of Records mentions only two theorems of mathematics. Pythagoras’ Theorem holds the record for the largest number of different proofs (about 350) and of course everybody has heard of Pythagoras’ Theorem, even if they can’t recall even one of these many proofs. But very few people have heard of the Classification Theorem for Finite Simple Groups. Its claim to fame is the sheer size of its proof. Nowhere does the proof appear in its entirety, and probably it will never appear complete in one publication. It is a mosaic of thousands of mathematical papers by hundreds of group theorists, all building on one another. If all the papers necessary for a complete proof were ever assembled in one place it is estimated that they would occupy about 15,000 pages (the equivalent of a large, multi-volume encyclopaedia)!

The theorem states that every finite simple group is either in one of 19 families or they are one of 15 sporadic or one-off examples.

Among the infinite families of finite simple groups are:
- $C_p$ for prime $p$ (these are the only finite abelian simple groups
- $A_n$ for $n \geq 5$, the alternating groups
- $PSL(n, p^m)$ for a prime $p$ and integers $m$ and $n$ where $n \geq 3$ or $n = 2$ and $q \geq 4$.

$PSL(n, p^m)$ is $SL(n, p^m)/H$ where $SL(n, p^m)$ is the group of all $n \times n$ matrices, with determinant 1, over the field $GF(p^m)$ of size $p^m$, and $H$ is its centre, the set of all $n \times n$ scalar matrices $\lambda I$ where $\lambda$ is an $n$’th root of unity.

There are 15 sporadic finite simple groups. These do not belong to one of the infinite families. The smallest of these is the Mathieu group $M_{11}$, of order 7920. The largest of these sporadic groups is called the Monster, with order $8080174247945128755886459904961710757005754368000000000 = 2^{46}3^{20}5^97^611^213^3.17.19.23.29.31.41.47.59.71$. Another is the so-called Baby Monster which only has order about $4 \times 10^{33}$. 


We now turn our attention to showing that $A_n$ is simple for $n \geq 5$. This fact is central to the insolubility of the quintic. Polynomials of degree 5 or more cannot be solved by radicals simply because $A_n$ is simple for $n \geq 5$.

**Theorem 2:** $A_n$ is generated by cycles of length 3.

**Proof:** Every even permutation is a product of an even number of transpositions. We show that any product of two transpositions $g = (x_1 \ x_2 \ x_3)(x_3 \ x_4)$ is a product of cycles of length 3.

**Case I:** the transpositions are disjoint: Then $g = (x_1 \ x_2 \ x_3)(x_1 \ x_4 \ x_3)$.

**Case II:** the transpositions have one symbol in common, say $x_4 = x_1$: Then $g = (x_1 \ x_2 \ x_3)$.

**Theorem 3:** If $n \geq 5$, all cycles of length 3 are conjugate in $A_n$.

**Proof:** Let $g = (x_1 \ x_2 \ x_3)$, $h = (y_1 \ y_2 \ y_3)$ be any two cycles of length 3. Then $g = k^{-1}hk$ for any permutation $k$ that maps $x_1$ to $y_1$, $x_2$ to $y_2$ and $x_3$ to $y_3$. With at least two more symbols to complete the definition it’s possible to arrange for $k$ to be even (just add a disjoint 2-cycle if necessary).

For $n < 3$ there are no cycles of length 3. For $n = 3$ or 4 there are two conjugacy classes of cycles of length 3 in $A_n$.

**Theorem 4:** $A_n$ is simple for $n \geq 5$.

**Proof:** Suppose that $n \geq 5$ and suppose that $H$ is a proper non-trivial normal subgroup of $A_n$. If $h \in H$ and $g \in A_n$ then, since $H$ is normal in $A_n$, $[g, h] = (g^{-1}h^{-1}g)h \in H$.

We’ll show that $H$ contains a cycle of length 3. Since all cycles of length 3 are conjugate to one another in $A_n$ this would mean that $H$ must contain every cycle of length 3 and so must contain every even permutation, contradicting the fact that $H < A_n$.

Choose $1 \neq h \in H$.

**Case 1:** $h = (xxxx\ldots)\ldots$: Without loss of generality we may let $h = (1234\ldots)\ldots$

Let $g = (123)$. Then $[g, h] = (132)(234) = (142)$.

**Case 2:** $h = (xxx)(xxx)\ldots$: Without loss of generality let $h = (123)(456)\ldots$ Let $g = (145)$. Then $[g, h] = (154)(256) = (16254)$. Go to case 1.

**Case 3:** $h = (xxx)(xxx)(xxx)\ldots$: Then $h^2 = (xxx)$. 

**Case 4:** $h = (xx)(xx)(xx)\ldots$: Without loss of generality let $h = (12)(34)(56)\ldots$ and let $g = (12345)$. Then $[g, h] = (15432)(21436) = (12453)$. Go to case 1.

**Case 5:** $h = (xx)(xx)$: Without loss of generality let $h = (12)(34)$ and let $g = (12345)$. Then $[g, h] = (15432)(21435) = (12453)$. Go to case 1.

In fact $A_n$ is simple for all values of $n$ except $n = 4$. For $n \leq 2$, $A_n$ is trivial. For $n = 3$ it is cyclic of order 3. And $A_4$ isn’t simple because it contains the proper, non-trivial, subgroup $V_4 = \{I, (12)(34), (13)(24), (14)(23)\}$.

Since $A_5$ is the smallest non-abelian simple group it is the smallest group that is not soluble.
§ 11.3. Metacyclic Groups

A metacyclic group $G$ is one that has a normal subgroup $H$ such that both $H$ and $G/H$ are cyclic. If $H = \langle A \rangle$ and $G/H$ is generated by the coset containing $B$, then $G$ is generated by $A$ and $B$.

Since $B^{-1} AB \in H$, $B^{-1} AB$ is a power of $A$, and hence so is $[A, B]$. Finally some power of $B$ will be in $H$. So a metacyclic group has the form:

$$G = \langle A, B \mid A^n, B^m = A^h, [A, B] = A^r \rangle$$

**Example 2:** Dihedral groups are metacyclic.

**Example 3:** $Q_8 = \langle A, B \mid A^4, B^2 = A^2, [A, B] = A^2 \rangle$ is the quaternion group. It, and $D_8$, are the two non-abelian groups of order 8.

Consider the metacyclic group $G = \langle A, B \mid A^n, B^m = A^h, [A, B] = A^r \rangle$

The commutator relation $[A, B] = A^r$ implies that $B^{-1} AB = A^{r+1}$ and so $AB = BA^{r+1}$.

Every time a $B$ moves left across an $A$ it is raised to the power $r + 1$.

Hence $A^s B = B A^{s(r+1)}$ and $A^n B^t = B A^{n(r+1)t}$.

In this way we can express any word in $A, B$ and the form $B^s A^t$ for some integers $s, t$.

Moreover, because of the power relator $B^h = A^h$ we can reduce $s$ modulo $m$ by replacing blocks of $m$ $B$'s by blocks of $h$ $A$'s.

And finally we can reduce the power of $A$ modulo $n$ because of the first power relator.

Every element of $G$ can be written in the form $B^s A^t$ where $0 \leq s < m$ and $0 \leq t < n$.

It would be possible to write the elements with the $A$'s coming before the $B$'s but we would need to convert the relation $B^{-1} AB = A^{r+1}$ into $B^{-(m-1)} AB^{m-1} = A^{(r+1)(m-1)}$ from which we would get $BB^{-m} AB^m B^{-1} = BAB^{-1} = A^{(r+1)(m-1)}$. Then, we could write $BA = A^{(r+1)(m-1)} B$.

However this is messier.

There are at most $mn$ distinct elements of the form $B^s A^t$ and hence $|G| \leq mn$. But in many cases the presentation will collapse, giving a smaller group, or even the trivial group.

**Example 4:** Let $G = \langle A, B \mid A^{60}, B^3 = A^4, [A, B] = A^6 \rangle$.

Then $B^{-1} AB = A^7$ and so $B^{-3} AB^3 = A^{43} = A^{43}$.

But $B^{-1} AB^3 = A^{-4} AA^4 = A$ and so $A^{43} = A$. Hence $A^{42} = 1$.

But the greatest common denominator of 42 and 60 is 6. This means that for some integers $h, k$, $42h + 60k = 6$. (We need not bother working out what these integers are.) It follows that $A^6 = A^{42h} A^{60k} = 1$.

So we can simplify the presentation to $\langle A, B \mid A^6, B^3 = A^4, [A, B] = 1 \rangle$. The group is abelian and has order at most 18. and can be written additively as $[A, B/6A = 0, 4A - 3B = 0]$ with matrix $\left( \begin{array}{cc} 6 & 0 \\ 4 & -3 \end{array} \right)$. Reducing this by elementary integer row and column operations we get:

$$\left( \begin{array}{cc} 2 & 3 \\ 4 & -3 \end{array} \right) \to \left( \begin{array}{cc} 2 & 3 \\ 0 & -9 \end{array} \right) \to \left( \begin{array}{cc} 2 & 3 \\ 0 & 9 \end{array} \right) \to \left( \begin{array}{cc} 2 & 1 \\ 0 & 9 \end{array} \right) \to \left( \begin{array}{cc} 1 & 2 \\ 9 & 0 \end{array} \right) \to \left( \begin{array}{cc} 1 & 0 \\ 9 & -18 \end{array} \right) \to \left( \begin{array}{cc} 1 & 0 \\ 0 & 18 \end{array} \right)$$.

Hence $G$ is none other than the cyclic group of order 18. (In fact $AB$ has order 18 and so is a generator.)

Recall that $\phi(n)$ denotes the order of the group $\mathbb{Z}_n^\#$. The elements of $\mathbb{Z}_n^\#$ are, modulo $n$, the integers that are coprime with $n$. 

214
Theorem 5: $G = \langle A, B | A^n, B^m = A^b, [A, B] = A^e \rangle$ is non-abelian of order $mn$ if and only if

1. $\gcd(r + 1, n) = 1$;
2. $d = \text{order of } r + 1 \text{ in } \mathbb{Z}_n$ is bigger than 1 and divides $D = \gcd(m, \varphi(n))$;
3. $n$ does not divide $r$;
4. $n$ divides $rh$.

Moreover, we may assume that $h$ divides $n$ in the sense that we may find a presentation of $G$ in which $h$ divides $n$.

**Proof:** Suppose $G$ is non-abelian and has order $mn$. Now $B^{-1}AB = A^{r+1}$.

1. Suppose $t > 1$ divides both $r + 1$ and $n$. Then $B^{-1}A^tB = A^{(r+1)t/n} = (A^n)^{(r+1)t/n} = 1$. Hence the order of $A$ divides $n/t$ and so $|G| \leq mn/t$. Hence $\gcd(r + 1, n) = 1$.
2. It follows that $r + 1 \in \mathbb{Z}_n$. Let $d$ be the order of $r$ in that group.

By Lagrange’s Theorem, $r + 1$ divides $\varphi(n)$.

Now $B^{-m}AB^m = A^{(r+1)m}$. But since $B^m$ is a power of $A$, we must have $A^{(r+1)m} = A$ and hence $A^{(r+1)m-1} = 1$. It follows that $(r + 1)m = 1$ in $\mathbb{Z}_n$ and so $d$ divides $m$, proving (2).

3. If $n$ divides $r$, $B^{-1}AB = A$ and so $G$ is abelian, a contradiction.
4. $B^{-1}A^hB = A^{r+1}h = A^h$ since $A^h$ is a power of $B$. Hence $A^{rh} = 1$ and so $n$ divides $rh$.

We omit the proof that if these conditions hold then $|G| = mn$.

Example 5: Find all the non-abelian metacyclic groups of order 30.

**Solution:**

Case 1: $n = 15, m = 2$: Then $\varphi(n) = 8$ and $D = 2$. Hence $d = 2$.

The elements of order 2 in $\mathbb{Z}_{15}$ are $r + 1 = \pm 4$ and $-1$ so $r = 3, -5$ or $-2$.

**Case 1A: $r = -2$:** $h = 15$ so $G_1 = \langle A, B | A^{15}, B^2, B^{-1}AB = A^{-1} \rangle$.

This is the dihedral group $D_{30}$.

**Case 1B: $r = -5, h = 3$:** $G_2 = \langle A, B | A^{15}, B^2 = A^{-5}, B^{-1}AB = A^4 \rangle$.

**Case 1C: $r = -5, h = 15$:** $G_3 = \langle A, B | A^{15}, B^2, B^{-1}AB = A^{-4} \rangle$.

**Case 1D: $r = 3, h = 5$:** $G_4 = \langle A, B | A^{15}, B^2 = A^5, B^{-1}AB = A^4 \rangle$.

**Case 1E: $r = 3, h = 15$:** $G_5 = \langle A, B | A^{15}, B^2, B^{-1}AB = A^{-4} \rangle$.

Case 2: $n = 10, m = 3$: Then $\varphi(n) = 4$ and $D = 1$. No such groups exist in this case.

Case 3: $n = 6, m = 5$: Then $\varphi(n) = 2$ and $D = 1$. No such groups exist in this case.

Case 4: $n = 5, m = 6$: Then $\varphi(n) = 4$ and $D = 2$. Hence $d = 2$.

The only element of order 2 in $\mathbb{Z}_5$ is $r + 1 = -1$, so $r = -2$. Clearly $h = 5$.

$G_6 = \langle A, B | A^5, B^6, B^{-1}AB = A^{-1} \rangle$.

Case 5: $n = 3, m = 10$: Then $\varphi(n) = 2$ and $D = 2$. Hence $d = 2$.

Again $r = -2$ and $h = 2$ and $G_7 = \langle A, B | A^3, B^{10}, B^{-1}AB = A^{-1} \rangle$.

Case 6: $n = 2, m = 15$: Then $\varphi(n) = 1$ and $D = 1$. No such groups exist in this case.

Although we get 7 groups of order 30 there are only three distinct groups among them:

$G_1, G_2 \cong G_3 \cong G_4 \cong G_6$ and $G_5 \cong G_7$.

§ 11.4. Power-Commutator Presentations

The presentation of a metacyclic group is an example of a power-commutator presentation.

A power-commutator presentation of a group is one of the form:

$$\langle A_1, \ldots, A_k | A_i^{n_i} = P_i \text{ for } i = 2, \ldots, k \text{ and } [A_i, A_j] = C_{ij} \text{ for } 0 \leq i < j \leq k \rangle$$
where each $P_i$ is a word in the generators up to $A_{i-1}$ (with $P_0 = 1$) and each $C_{ij}$ is a word in the generators up to $A_{j-1}$.

We can write every element of such a group in the form $A_k a_k A_k^{-1} a_k^{-1} \ldots A_1 a_1$ where $0 \leq a_i < n_i$ for each $i$. The reason for the reverse order is because $A_i A_j = A_j A_i C_{ij}$ for all $i < j$ and so writing the generators in reverse order is more convenient.

Given a word in the generators we bring all the $A_k$'s to the left using the relations $A_i A_k = A_k A_i C_{ij}$. The word to the right of this power of $A_k$'s involves only the generators up to $A_{k-1}$. We now bring all the $A_{k-1}$'s to the left, immediately to the right of the $A_k$'s. We continue in this way.

The order of such a group is at most $n_1 n_2 \ldots n_k$, but it can be smaller. Let us consider the special cases where the number of generators is small.

**One Generator:** A power-commutator presentation in one generator will have the form $G = \langle A \mid A^n = 1 \rangle$ and so the group will be a finite cyclic group. Clearly $G' = 1$ in this case.

**Two Generators:** A power-commutator in 2 generators will have the form:

$$G = \langle A, B \mid A^m = 1, B^n = A^k, [A, B] = A^r \rangle$$

and so the group will be metacyclic. Clearly $G'' = 1$ in this case.

**Three Generators:** A power-commutator in 3 generators will have the form:

$$\langle A, B, C \mid A^m = 1, B^n = A^k, C^d = B^e A^f, [A, B] = A^r, [A, C] = B^h A^k, [B, C] = B^u A^v \rangle$$

The subgroup $H = \langle A, B \rangle$ will be normal, since $C^{-1}AC = AB^h A^k$ and $C^{-1}BC = B^{u+1} A^r$.

$H$ will contain a normal subgroup $K = \langle A \rangle$, which may not be normal in $G$. Since $G/H$, $H/K$ and $K$ are cyclic, $G''' = 1$. The soluble length of $G$ is thus at most 3 (but it could be less).

**Example 6:** Let $G$ be the group


Write the product $(DCBA)(D^2CA^3)$ in the form $D^p C^q B^r A^s$ where $0 \leq p < 3, 0 \leq q < 2, 0 \leq r < 2$ and $0 \leq s < 4$.

[Here, to save space, we omit commutators where generators commute.]

**Solution:** From the power relations we have:

(P1) $A^4 = 1$;
(P2) $B^2 = A^2$;
(P3) $C^2 = A^2$;
(P4) $D^3 = 1$.

From the commutator relations we have:

(C1) $AB = BA$; $AC = CA$; $AD = DA$;
(C2) $BC = CBA^2$;
(C3) $BD = DBCA^2 = DCB^2 A^2 = DCA^2$;
(C4) $CD = DCBA^2$.

Hence $(DCBA)(D^2CA^3) = (DCBD^2C)A^4$ by C1

$$= D(C(BD)DC)$$

$$= DC(DCA^2)DC \text{ by C3}$$

$$= (DCDCDC)A^2 \text{ by C1}$$

$$= (CD)(CD)CA^2$$

$$= D(CDCA^2)(DCBA^2)CA^2 \text{ by C4}$$

$$= (D^2CBDCBC)A^6 \text{ by C1}$$
What is |G|

However we can do better than that.

Hence |G| divides 60.

Example 8: $G = \langle A, B, C | A^4, B^4, C^2, [A, C] = B^2 \rangle$. This group has order 32 and its elements are of the form $C^i B^j A^k$ where $i, j, 0, 1, 2, 3$ and $k = 0, 1$.

Since $[A, C] = B^2, AC = CAB^2$. So every time a $C$ moves to the left across an $A$, a factor of $B^2$ is introduced. Since both $B$ is in the centre the $A$s and $B$'s can be brought to the right.

A typical product is $C^i B^j A^k \times C^s B^t A^w = C^{i+s} B^{2uk+jv} A^{k+w}$. (We introduce $uk$ factors of $B^2$ because we have to move a $C$ past an $A$ $uk$ times.)

For example $C^2 B A^2 \times C^3 B^2 A^2 = C^3 B^{12+1+3} A^4 = C^3 B^{16} A^4 = C$.

The bottom-right hand portion of the group table is:

<table>
<thead>
<tr>
<th></th>
<th>CBA^3</th>
<th>CB^2</th>
<th>CB^2A</th>
<th>CB^2A^3</th>
<th>CB^3</th>
<th>CB^3A</th>
<th>CB^3A^2</th>
<th>CB^3A^3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBA^3</td>
<td>A^2</td>
<td>BA^3</td>
<td>B</td>
<td>BA</td>
<td>BA^2</td>
<td>B^2</td>
<td>B^2A</td>
<td>B^2A</td>
</tr>
<tr>
<td>CB^2</td>
<td>B^A^3</td>
<td>1</td>
<td>A</td>
<td>A^2</td>
<td>A^3</td>
<td>B</td>
<td>BA</td>
<td>BA^3</td>
</tr>
<tr>
<td>CB^3</td>
<td>A^2</td>
<td>B</td>
<td>BA</td>
<td>BA^2</td>
<td>BA^3</td>
<td>B^2</td>
<td>B^2A</td>
<td>B^2A</td>
</tr>
<tr>
<td>CB^3A</td>
<td>B^2</td>
<td>B^A</td>
<td>B^3A</td>
<td>B^3A^2</td>
<td>B^3</td>
<td>A</td>
<td>A^2</td>
<td>A^3</td>
</tr>
<tr>
<td>CB^3A^2</td>
<td>A</td>
<td>BA^2</td>
<td>BA^3</td>
<td>B</td>
<td>BA^2</td>
<td>B^2A^2</td>
<td>B^2A</td>
<td>B^2A</td>
</tr>
<tr>
<td>CB^3A^3</td>
<td>B^2A</td>
<td>B^A</td>
<td>B^3</td>
<td>B^A</td>
<td>BA^2</td>
<td>A</td>
<td>1</td>
<td>A</td>
</tr>
</tbody>
</table>

Example 7:


What is $|G|$?

Solution: $\text{GCD}(60, 9) = 3$ so $A^3 = 1$.

$\text{GCD}(10, 2^4 - 1) = 5$ so $B^5 \in \langle A \rangle$.

Hence $|G|$ divides 60.

However we can do better than that.
Since \( C^{-1}AC = A^{15} = 1 \), we have \( A = 1 \).
\( C^{-1}BC = B^2A = B^2 \). Cubing both sides we get \( C^{-1}B^3C = B^6 \).
But \( B^3 = C^4 \) so \( C^{-1}B^3C = B^3 \).
Hence \( B^6 = B^3 \) and so \( B^3 = 1 \).
However \( B^5 \in \langle A \rangle = 1 \) so \( B^{\gcd(3, 5)} = 1 \) whence \( B = 1 \).
So \( G = \langle C \mid C^4 \rangle \) and so \( |G| = 4 \).

§ 11.5. Power-Commutator Presentations and Soluble Groups

**Theorem 6:** The group \( G \) has a power-commutator presentation if and only if it is a finite soluble group.

**Proof:** Suppose \( G \) has the presentation:
\[
\langle A_1, \ldots, A_k \mid A_i^{m_i} = P_1 (A_1, \ldots, A_{i-1}) \text{ for } i = 1, \ldots, k, [A_i, A_j] = C_{ij}(A_1, \ldots, A_{i-1}) \text{ for } 0 \leq i < j \leq k \rangle.
\]
For \( r = 1, 2, \ldots, k \) let \( G_r = \langle A_1, \ldots, A_r \rangle \) be the subgroup generated by the first \( r \) generators.
Suppose \( r > 1 \). For \( i < r \), \( [A_i, A_r] \in G_{r-1} \) and so it follows that \( G_r' \leq G_{r-1} \). Also \( G_1' = 1 \). Hence \( G \) is soluble of length at most \( k \).

Conversely suppose \( G \) is a finite soluble group. By induction we may suppose that \( G' \) has a power-commutator presentation:
\[
\langle A_1, \ldots, A_k \mid A_i^{m_i} = P_1 (A_1, \ldots, A_{i-1}) \text{ for } i = 1, \ldots, k, [A_i, A_j] = C_{ij}(A_1, \ldots, A_{i-1}) \text{ for } 0 \leq i < j \leq k \rangle.
\]
Now \( G/G' \) is a finite abelian group. Let \( G/G' \) be generated by the cosets \( B_1G', \ldots, B_sG' \).
Clearly \( G \) is generated by \( \{A_1, \ldots, A_k, B_1, \ldots, B_s\} \). Now if the coset \( B_iG' \) has order \( m_i \) then \( B_i^{m_i} \in G' \) and so \( B_i^{m_i} \in \langle A_1, \ldots, A_k \rangle \).

For \( i = 1, \ldots, k \) and \( j = 1, \ldots, s \) we have \( [A_i, B_j] \in G' \) whence \( [A_i, B_j] \in \langle A_1, \ldots, A_k \rangle \).
Similarly for \( 1 \leq i < j \leq s \) we have \( [B_i, B_j] \in G' \) whence \( [B_i, B_j] \in \langle A_1, \ldots, A_k \rangle \).
This leads to a power-commutator presentation for \( G \).
EXERCISES FOR CHAPTER 11

EXERCISE 1: For each of the following statements determine whether it is true or false.
(1) The derived subgroup is the set of all commutators.
(2) The inverse of a commutator is a commutator.
(3) A conjugate of a commutator is a commutator.
(4) The product of two commutators is a commutator.
(5) $G/G'$ is always abelian.
(6) $S_n$ is a simple group for all $n$.
(7) If $G$ is a non-abelian simple group $G' = G$.
(8) $A_n$ is simple for all $n$.
(9) If $G = \langle A, B \mid A^{-1}BA = A^3B \rangle$ then $(AB)^3 = A^{21}B^3$.
(10) All groups whose order is less than 60 are soluble.

EXERCISE 2: If $G = \langle A, B \mid A^{26} = B^3 = 1, [A, B] = A^2 \rangle$ find the order of $BA$.

Express $(BA)^3$ in the form $C^mB^nA^t$.

EXERCISE 4: Let $G = \langle A, B, C \mid A^{10} = B^6 = C^8 = 1, [A, B] = C, [A, C] = [B, C] = 1 \rangle$.
(a) Show by induction that $B^{-n}AB = AC^n$ for all $n$.
(b) Find $|G|$.
(c) Find $|Z(G)|$.
(d) Find $|G'|$.

EXERCISE 5:
Let $G = \langle A, B, C \mid A^m = 1, B^n = A^k, C^d = B^sA^t, [A, B] = A^l, [A, C] = A^s, [B, C] = B^uA^v \rangle$.
Show that $A^M = 1$ where $M = \text{GCD}(m, (r + 1)\text{GCD}(n, u) - 1)$ and $B^{MT} = 1$ where
$T = \text{GCD}(n, (u + 1)d - 1)$.

EXERCISE 6:
Let $G = \langle A, B \mid A^n, B^m = A^h, [A, B] = A^i \rangle$ be a metacyclic group.
Find $Z(G)$ and $G'$.

SOLUTIONS FOR CHAPTER 11

EXERCISE 1: (1) FALSE (it is the subgroup generated by all the commutators); (2) TRUE; (3) TRUE; (4) FALSE; (5) TRUE; (6) FALSE (A_n is a normal subgroup); (7) TRUE; (8) FALSE (A_4 has V_4 as a proper, non-trivial normal subgroup); (9) TRUE; (10) TRUE.

Hence $(BA)^2 = BAB\bar{A} = B^2A^4$ and
$(BA)^3 = BAB^2A^3 = B^3A^6A^4 = B^3A^{13} = A^{13}$.
Hence $(BA)^6 = A^{26} = 1$, so $BA$ has order 6.
$AB$ always has the same order as $BA$ and so it too has order 6.
EXERCISE 3: Since \([A, B] = C, AB = BAC\). Since \(C\) commutes with both \(A\) and \(B\), 
\(AB = CBA\).
So \((BA)^3 = B(AB)A = B(CBA)A = CB^2A^2\).
And \((BA)^3 = (BA)CB^2A^2 = CB(AB)BA^2 = CB(CBA)BA^2 = C^2B^2(AB)A^2 = C^2B^2(CBA)A^2 = C^3B^3A^3\).

EXERCISE 4: (a) Since \(A^{-1}B^{-1}AB = C, B^{-1}AB = AC\), so it holds for \(n = 1\).
Suppose \(B^{-n}AB^n = AC^n\). Then \(B^{-1}(B^{-n}AB^n)B = B^{-1}AC^nB = ACC^n = AC^{n+1}\).
(b) Since \(B^6 = 1, A = B^{-6}AB^6 = AC^6\) so \(C^6 = 1\). Since \(C^8 = 1\) it follows that \(C^2 = 1\).
(c) \(|G| = 120\) since every element can be expressed uniquely as \(A^mB^nC^r\) where \(m = 0, 1, 2, \ldots, 9, n = 0, 1, 2, \ldots, 5, r = 0, 1, 2\).
(d) Clearly \(C \in Z(G)\). Also, \(B^2AB^2 = AC^2 = A\) so \(B^2 \in Z(G)\). And \(B^{-1}A^2B = (AC)^2 = A^2C^2\) so \(A^2 \in Z(G)\). Hence \(Z(G) = \{A^2m, B^2n, C\}\) which has order \(5 \times 3 \times 2 = 30\).
(e) \(G' = \langle C \rangle\) so \(|G'| = 2\).

EXERCISE 5: Since \(B^n = A^k\), it follows that \(B^n\) commutes with \(A\).
Since \((BC)^{-1}A(BC) = A^{(r+1)(s+1)} = (CB)^{-1}A(CB)\) it follows that \([B, C] = (CB)^{-1}(BC)\) commutes with \(A\). Hence \(B^nA^r\) commutes with \(A\) and so \(B^n\) commutes with \(A\).
It follows that \(B^{|GCD(n, u)}\) commutes with \(A\).
Conjugating \(A\) by \(B^{|GCD(n, u)}\) gives \(A^{(r+1)^{|GCD(n, u)}}}\).
So \(A^{(r+1)^{|GCD(n, u)}}} = A\) and so if \(P = (r + 1)^{|GCD(n, u)} - 1, A^p = 1\).
But \(A^m = 1\) and so \(A^{|GCD(n, p)} = 1\).
Let \(H = \langle A \rangle\). Then \(G/H\) has the presentation \(\langle B, C \mid B^n = 1, C^d = B^e, [B, C] = B^v \rangle\) and so by
the first part applied to \(G/H, B^T \in H\) where \(T = \text{GCD}(n, (u + 1)^k - 1)\).
Hence \(B^HT = 1\).

EXERCISE 6: Suppose \(A'B' \in Z(G)\).
Then \(A^{-1}(A'B')A = A'B'\) and so \(A^{-1}B'A = B'\), whence \(B' \in Z(G)\).
Similarly \(A' \in Z(G)\).
Now \(B'AB = A'^{r+1}\) so \(B^{-1}A'B = A^{(r+1)^i} = A^i\) and so \(A'^i = 1\).
Hence \(n \mid r\) and so \(A' \in \langle A'^{|GCD(n, r)}\rangle\). Conversely \(A'^{|GCD(n, r)} \in Z(G)\).
Also \(B'^{-j}AB = A^{(r+1)^j}\).
Hence \(B'^{-1}A^{-1}B' = A^{-(r+1)^j}\) and so \(A'^{-1}B' = B'^{-(r+1)^j}\).
Hence \(A'^{-1}B'A = B'^{-(r+1)^j}B' = B'^j\), so \(A^{1-(r+1)^j} = 1\). Hence \(n \mid (r + 1)^j - 1\) and so if \(d\) is the order of \(r + 1\) in \(Z_m^\#\) then \(d \mid j\). Hence \(B' \in \langle B'^d \rangle\). Conversely \(B'^d \in Z(G)\).
Hence \(Z(G) = \langle A'^{|GCD(n, r)} \rangle, B'^d \rangle\) where \(d\) is the order of \(r + 1\) in \(Z_m^\#\).

\([A, B] = A'\) so \(G'\) contains \(A'\).
Let \(H = \langle A' \rangle\). Then \(H \leq G'\).
In \(G/H, [AH, BH] = [A, B]H = H\) so \(G/H\) is abelian and so \(G' \leq H\).
Hence \(G' = \langle A' \rangle\).