3. METACYCLIC GROUPS

§ 3.1. Polycyclic Groups

The class of **polycyclic groups** is $\mathcal{C}^{\infty}$. So a group is polycyclic if and only if, for some n, there is a subnormal series

$$1 = G_0 < G_1 < \dots < G_n = G$$

Where each G_{i+1}/G_i is cyclic.

Clearly polycyclic groups are soluble. Does the converse hold? Clearly not, otherwise it would be a bit silly to have two names for the same class of groups.

Theorem 1: Subgroups and quotient groups of polycyclic groups are polycyclic. Moreover, if H and G/H are polycyclic then so is G.

Proof: This follows from Theorem 2 of Chapter 1. ✋☺

Theorem 2: All finite soluble groups are polycyclic.
Proof: Suppose G is finite and soluble. Then there is a subnormal series from 1 to G where the quotients are finite and abelian. Since finite abelian groups are direct sums of finite cyclic groups they are polycyclic and so they belong to $(\mathcal{C}^\infty)^\infty = \mathcal{C}^\infty$. ✋☺

In fact all finitely generated soluble groups are polycyclic. To find our soluble group that's not polycyclic we must look among soluble groups that are not finitely generated.

Example 1: $\mathbf{C}_2 \times \mathbf{C}_2 \times \ldots$ is soluble but not polycyclic. Remember that a subnormal series must be finite.

§ 3.2. Metacyclic Groups

The classes of soluble and polycyclic groups are very large, so large that we could never classify their groups. Here we'll focus on a class of polycyclic groups, $\mathcal{C}^2$, that is just a bit wider than the class $\mathfrak{D}$ of cyclic and dihedral groups. So we have:

$\mathfrak{D} \subseteq \mathcal{C}^2 \subseteq \mathcal{C}^\infty \subseteq \mathfrak{S}$, that is

cyclic/dihedral $\rightarrow$ metacyclic $\rightarrow$ polycyclic $\rightarrow$ soluble.

The class of **metacyclic groups** is defined to be $\mathcal{C}^2$.

Thus a group G is metacyclic if and only if it has a normal subgroup H such that both H and G/H are cyclic.

Example 2: The group $\mathbf{A}_4$ is polycyclic but not metacyclic.
The subnormal series $\mathbf{1} < \langle(12)(34)\rangle < \mathbf{V}_4 < \mathbf{A}_4$ has cyclic quotients $\mathbf{C}_2$, $\mathbf{C}_2$ and $\mathbf{C}_3$ so A_4 is polycyclic.

If it was metacyclic it would have to have a subnormal series:

$$\mathbf{1} < H < \mathbf{A}_4$$

where H and $\mathbf{A}_4$/H are cyclic.

Case I: $\mathbf{H \cong C_6}$: Then H must contain an element of order 6 which must have cycle structure (×××)(××) … and this would require at least 5 symbols.

Case II: $\mathbf{H \cong C_4}$: Then H must contain an element of order 4 which must have cycle structure (××××). But such a permutation is odd.

Case III: $\mathbf{H \cong C_3}$: Then G/H must be isomorphic to $\mathbf{C}_4$ and be generated by an element of order 4. Then $\mathbf{A}_4$ must have an element whose order is divisible by 4, which is not the case.

Case IV: $H \cong C_2$: Then G/H must be isomorphic to $\mathbf{C}_6$ and be generated by an element of order 6. Then A_4 must have an element whose order is divisible by 6, which is not the case.

§ 3.3. The Structure of Metacyclic Groups

Theorem 2: Metacyclic groups have the form:

$$M(m, n, h, r) = \langle A, B \mid A^m, B^n = A^h, B^{-1}AB = A^r \rangle$$

for some integers m, n, h and r.

Proof: Suppose G is metacyclic. Then there exists a cyclic normal subgroup H such that G/H is 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. Finally some power of B will be in H. So a metacyclic group has the form:

$$\langle A, B \mid A^m, B^n = A^h, B^{-1}AB] = A^r \rangle.$$ ✋☺

Examples 3: Dihedral groups are metacyclic.
$\mathbf{Q}_8 = \langle A, B \mid A^4, B^2 = A^2, [A, B] = A^2 \rangle$ is the quaternion group. It, and $\mathbf{D}_8$, are the two non-abelian groups of order 8 and both are metacyclic.

Consider the metacyclic group

$$M(m, n, h, r) = \langle A, B \mid A^m, B^n = A^h, B^{-1}AB = A^r \rangle$$

Since $B^{-1}AB = A^r$ we have $AB = BA^r$. Every time a B moves left across an A it's raised to the power r.

Hence $A^uB = BA^{ur}$ and so $A^uB^v = B^vA^{ur^v}$.

In this way we can express any word in A, B in the form B^sA^t for some integers s, t. Moreover, because of the power relator $B^m = A^h$ we can reduce s modulo n by replacing blocks of n B's by blocks of h A's.

And finally we can reduce the power of A modulo m because of the first power relator. Every element of G can be written as B^sA^t where $0 \le s < n$ and $0 \le t < m$.

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

There are at most mn distinct elements of the form B^sA^t and so $|G| \le mn$. 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 $B^{-3}AB^3 = A^{7^3} = A^{343} = A^{43}$.
But $B^{-3}AB^3 = A^{-4}AA^4 = A$ 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 needn't 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 = 4A – 3B = 0] with matrix $\begin{pmatrix} 6 & 0 \\ 4 & -3 \end{pmatrix}$. Reducing this by elementary integer row and column operations we get:

$$\begin{pmatrix} 2 & 3 \\ 4 & -3 \end{pmatrix} \to \begin{pmatrix} 2 & 3 \\ 0 & -9 \end{pmatrix} \to \begin{pmatrix} 2 & 3 \\ 0 & 9 \end{pmatrix} \to \begin{pmatrix} 2 & 1 \\ 0 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 9 & 0 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 \\ 9 & -18 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 18 \end{pmatrix}.$$

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

§ 3.4. Enumerating Metacyclic Groups

Theorem 3: The abelian metacyclic groups of order N are those of the form $\mathbf{C}_m \times \mathbf{C}_n$ where $mn = N$.

Proof: Let G be an abelian metacyclic group of order N. Then G has the form:

$$M(m, n, h, 1) = \langle A, B \mid A^m, B^n = A^h, BA = AB\rangle$$

Theorem 4: The non-abelian metacyclic groups of order N have the form:

$$M(m, n, h, r) = \langle A, B \mid A^m, B^n = A^h, B^{-1}AB = A^r\rangle$$

where:

(1) $mn = N$;
(2) $2 < m < N$;
(3) $h > 1$ and h divides m;
(4) r is coprime to m;
(5) m divides $h(r - 1)$;
(6) m divides $r^n - 1$.

Proof:

Suppose that $G = \langle A, B \mid A^m, B^n = A^h, B^{-1}AB = A^r \rangle$ is non-abelian of order N.

(1) We have shown that $N = mn$.

(2) If $m = 1$ then $G = \langle B \rangle$ and so is cyclic.
If $m = 2$ then $r = 1$ and so G is abelian.
If $m = N$ then $G = \langle A \rangle$ and so is cyclic.
Hence $1 < m < N$.

(3) If $h = 1$ then $G = \langle B \rangle$ and so is cyclic. Hence $h > 1$.

(4) $B^{-1}AB = A^r$. Let $d = GCD(r, m)$ and suppose that $d > 1$. Let $s = r/d$ and $t = m/d$.
Then $B^{-1}A^tB = A^{rt} = A^{dst} = A^{ms} = 1$.
Hence $A^t = 1$, yet $t < m$, a contradiction. Hence $d = 1$ and so r, m are coprime.

(5) $B^{-1}AB = A^r$ so $B^{-1}A^hB = A^{rh}$.
Since $A^h = B^n$, $A^{rh} = A^h$ and so $A^{h(r-1)} = 1$.
Hence m divides $h(r - 1)$.

(6) $B^{-1}AB = A^r$ so $B^{-n}AB^n = A^{r^n}$.
Since $B^n = A^h$, $A^{r^n} = A$ and so m divides $r^n - 1$.
I omit the proof of the fact that if all these conditions hold then the group so presented has order N. ✋☺

To find all the non-abelian metacyclic groups of order N:
(1) Choose m dividing N with $2 < m < N$.
(2) Let $n = N/m$.
(3) Choose $h > 1$, dividing m.
(4) Choose $r > 1$ such that:

   (a) r is coprime to m;
   (b) m divides $h(r - 1)$;
   (c) m divides $r^n - 1$.

Then $M(m, n, h, r)$ is a non-abelian metacyclic group of order N.

Keep in mind that different presentations of metacyclic groups can give the same group. For example, r can be replaced by any integer that is coprime to m since A can be replaced by A^t for any t that's coprime to m. Also, sometimes the relation $B^n = A^h$ can be replaced by one where $A^h = 1$ by making changes to the generators.

Example 4: Find all the non-abelian metacyclic groups of order 8.
Solution: N = 8. The possibilities are found in the following table:

m	*n*	*h*	*r*	G
4	2	2	3	$\mathbf{Q}_8$
4	2	4	3	$\mathbf{D}_8$

These are the only non-abelian metacyclic groups of order 8. In fact they are the only non-abelian groups of order 8.

Example 5: Find all the non-abelian metacyclic groups of order 20.
Solution: N = 20. The possibilities are found in the following table:

m	*n*	*h*	*r*	G
4	5	2	none	
4	5	4	none	
5	4	5	2	G_1
5	4	5	3	G_2
5	4	5	4	G_3
10	2	2	none	
10	2	5	9	G_4
10	2	10	9	G_5

$G_1 \cong \langle A, B \mid A^5, B^4, B^{-1}AB = A^2\rangle$
$G_2 \cong \langle A, B \mid A^5, B^4, B^{-1}AB = A^3\rangle$
$G_3 \cong \langle A, B \mid A^5, B^4, B^{-1}AB = A^{-1}\rangle$
$G_4 \cong \langle A, B \mid A^{10}, B^2 = A^5, B^{-1}AB = A^{-1}\rangle$
$G_5 \cong \langle A, B \mid A^{10}, B^2, B^{-1}AB = A^{-1}\rangle \cong \mathbf{D}_{20}$.

Now $G_1 \cong G_2$ [let C = A^2] and $G_3 \cong G_4$ [let C = A^2].
So in fact there are only 3 non-abelian metacyclic groups of order 20. In fact these are the only non-abelian groups of order 20.

Theorem 5: Let $G = \langle A, B \mid A^m, B^n = A^h, B^{-1}AB = A^r\rangle$ be a metacyclic group. Let $d = \mathrm{GCD}(m, r-1)$.
Then $Z(G) = Z(G) = \langle A^{m/d}, B^k\rangle$ where k is the order of r in $\mathbb{Z}_m^{\#}$ and $G' = \langle A^{r-1}\rangle$.

Proof:

Suppose $A^iB^j \in Z(G)$.
Then $A^{-1}(A^iB^j)A = A^iB^j$ and so $A^{-1}B^jA = B^j$,
Whence $B^j \in Z(G)$.
Similarly $A^i \in Z(G)$.
Now $B^{-1}AB = A^r$ so $B^{-1}A^iB = A^{ri} = A^i$
and so $A^{i(r-1)} = 1$.
Hence $m \mid i(r-1)$.
Let $m = du$ and $r - 1 = dv$ where u, v are coprime.
Then $du \mid dvi$ and so $u \mid vi$. Since u, v are coprime, $u \mid i$ and so $A^i \in \langle A^u\rangle = \langle A^{m/k}\rangle$.
Conversely $A^{m/k} \in Z(G)$.
Also $B^{-j}AB^j = A^{r^j}$. $\therefore$ $B^{-j}A^{-1}B^j = A^{-r^j}$ and so $A^{-1}B^j = B^jA^{-r^j}$. Thus $A^{-1}B^jA = B^jA^{1-r^j} = B^j$, so $A^{1-r^j} = 1$.
So $m \mid r^j - 1$ and so if k is the order of r in $\mathbb{Z}_m^{\#}$ then $k \mid j$.
Hence $B^j \in \langle B^k\rangle$. Conversely $B^k \in Z(G)$.
Hence $Z(G) = \langle A^{m/d}, B^k\rangle$.

$[A, B] = A^r$ so G' contains A^r.
Let $H = \langle A^r \rangle$. Then $H \leq G'$.
In G/H, $[AH, BH] = [A, B]H = H$ so G/H is abelian and so $G' \leq H$. Hence $G' = \langle A^r \rangle$. ✋☺

EXERCISES FOR CHAPTER 3

Exercise 1: For each of the following statements determine whether it is true or false.
(1) All polycyclic groups are soluble.
(2) All soluble groups are polycyclic.
(3) Metacyclic groups all have the form:

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

(4) The order of the group $\langle A, B \mid A^m, B^n, [A, B] = A^r\rangle$ can be less than mn.
(5) $\mathbf{A}_5$ is the smallest non-metacyclic group.

Exercise 2: Find all the metacyclic groups of order 30.

Exercise 3: If $G = \langle A, B \mid A^{26}, B^3, B^{-1}AB = A^3\rangle$ find the order of BA.

Exercise 4: Let $G = \langle A, B \mid A^{16}, B^4 = A^4, B^{-1}AB = A^{13}\rangle$. Find Z(G) and G′.

SOLUTIONS FOR CHAPTER 3

Exercise 1:
(1) TRUE
(2) FALSE: There are infinite soluble groups that aren't polycyclic.
(3) FALSE: $\mathbf{Q}_8$ the quaternion group:
$\langle A, B \mid A^4, B^2 = A^2, [A, B] = A^2\rangle$ is metacyclic but doesn't have a presentation of this form.

(4) FALSE: Let G = $\langle A, B \mid A^3, B^2, [A, B] = A^2 \rangle$.
Then $B^{-1}AB = A^3 = 1$ and so A = 1. This group is therefore just $\mathbf{C}_2$.
(5) FALSE: $\mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2$ is the smallest non-metacyclic group.

Exercise 2:
We begin with the abelian metacyclic groups of order 30. Every finite abelian group is a direct product of cyclic groups of prime-power order. So the only abelian group of order 30 is: $\mathbf{C}_2 \times \mathbf{C}_3 \times \mathbf{C}_5$ which is $\mathbf{C}_{30}$.
So $\mathbf{C}_{30}$ is the only abelian metacyclic group of order 30.

Now we consider the non-abelian metacyclic groups of order 30.

m	***n***	***h***	***r***	**G**
2	15	2	none	
3	10	3	2	$\mathbf{D}_6 \times \mathbf{C}_5$
5	6	5	4	$\mathbf{D}_{10} \times \mathbf{C}_3$
15	2	5	4	$\mathbf{D}_{10} \times \mathbf{C}_3$
15	2	15	4	$\mathbf{D}_6 \times \mathbf{C}_5$
15	2	15	11	$\mathbf{D}_{10} \times \mathbf{C}_3$
15	2	15	14	$\mathbf{D}_{30}$

So the metacyclic groups of order 30 are:
$\mathbf{C}_{30}$, $\mathbf{D}_{30}$, $\mathbf{D}_6 \times \mathbf{C}_5$ and $\mathbf{D}_{10} \times \mathbf{C}_3$.

Exercise 3: Since $[A, B] = A^2$, $BA = A^3B$.

Hence $(BA)^2 = BABA = B^2A^4$ and
$(BA)^3 = BAB^2A^4 = B^3A^9A^4 = B^3A^{13} = A^{13}$.
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 4: $m = 16$, $n = 4$, $h = 4$, $r = 13$, $d = 4$, $k = 4$
So $Z(G) = \langle A^{16/4}, B^4\rangle = \langle A^4, B^4\rangle = \langle A^4\rangle$ and $\langle A^{12}\rangle = \langle A^4\rangle$
$G' = \langle B^{12}\rangle = \langle A^{12}\rangle = \langle A^4\rangle$.