1
The elements

Here we shall introduce our principal objects of study, the polycyclic groups, and derive some of their simpler properties. The main purpose of the chapter is to illustrate the use of a variety of quite elementary techniques which play a humble but necessary role in this subject.

A. The maximal condition and solubility

Definition A group G has *max* if one of the following holds:

(*a*) every family of subgroups of G has a maximal member;
(*b*) every strictly ascending chain of subgroups of G is finite;
(*c*) every subgroup of G is finitely generated.

Exercise 1 Prove that (*a*), (*b*) and (*c*) are equivalent. (This is really universal algebra. Use Zorn's Lemma for '$(b) \Rightarrow (a)$'.)

Proposition 1 Suppose $N \lhd G$. Then G has *max* if and only if both N and G/N have *max*.

Proof 'Only if' is very easy. For the converse, consider an ascending chain $(H_i)_{i \in \mathbb{N}}$ of subgroups of G; that is, $H_1 \leq H_2 \leq \ldots \leq G$. If N and G/N have *max*, than there exists $n \in \mathbb{N}$ such that $H_i \cap N = H_n \cap N$ and $H_i N = H_n N$ for all $i \geq n$. We deduce that $H_i = H_n$ for all $i \geq n$ and the conclusion is that G has *max*. (The deduction goes like this: suppose $i \geq n$; then

$$\begin{aligned} H_i = H_i \cap (H_i N) &= H_i \cap (H_n N) \\ &= H_n(H_i \cap N) \text{ by the modular law, since } H_i \geq H_n \\ &= H_n(H_n \cap N) = H_n.) \end{aligned}$$

Examples of groups having *max*:

(*a*) finite groups;
(*b*) C_∞, the infinite cyclic group.

Until recently, the only known groups with *max* were those built up from (*a*) and (*b*) using Proposition 1. In 1978, E. Rips and A. Yu. Ol'shanskii independently announced the construction of infinite simple groups having both *max* and *min* (every descending chain of subgroups is finite). These groups are both complex and mysterious, and we shall say no more about this development. Instead we concentrate on the groups mentioned above, the *polycyclic-by-finite* groups. The reason for this name will shortly become clear.

Suppose $\mathscr{P}$ is a property of groups. A group G is called poly-$\mathscr{P}$ if there exists a finite chain of subgroups

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_{n-1} \lhd G_n = G \qquad (1)$$

such that each of the factor groups G_i/G_{i-1} has the property $\mathscr{P}$.

Let $\mathscr{Q}$ be another property of groups. A group G is a $\mathscr{P}$-by-$\mathscr{Q}$ group if G has a normal subgroup N such that N has $\mathscr{P}$ and G/N has $\mathscr{Q}$.

Proposition 2 The following properties of a group are equivalent:

(*a*) poly-(cyclic or finite);
(*b*) polycyclic-by-finite;
(*c*) (poly-C_∞)-by-finite.

Here 'polycyclic' means 'poly-cyclic', and 'poly-C_∞' is short for 'poly-(infinite cyclic or trivial)'. Obviously $(c) \Rightarrow (b)$ and $(b) \Rightarrow (a)$. To show that $(a) \Rightarrow (c)$ we make some preliminary observations.

Lemma 1 Let H be a finitely generated group and B a finite group. Then H has only finitely many normal subgroups N with $H/N \cong B$.

Proof There are only finitely many distinct homomorphisms of H onto B, since there are at most $|B|$ possible images for each of the finitely many generators of H. The result now follows from the fact that every $N \lhd H$ with $H/N \cong B$ arises as the kernel of such a homomorphism.

Lemma 2 Suppose H is a finitely generated group and $K \lhd_f H \lhd G$ for some group G. Then K has a subgroup K^0 of finite index with $K^0 \lhd G$.

Proof If $g \in G$ then $K^g \lhd H$ and $H/K^g \cong H/K$. By Lemma 1 there are only finitely many distinct groups among the K^g as g runs through G; call them $K_1, \ldots, K_n$. Then $K^0 = K_1 \cap \ldots \cap K_n$ is normal in G and has index at most $|H:K|^n < \infty$ in H.

Lemma 3 Suppose a group A has a finite normal subgroup B such that $A/B \cong C_\infty$. Then A has an infinite cyclic normal subgroup of finite index.

Proof We have $A = B\langle x \rangle$ for some $x \in A$. Since B is finite, so is Aut B. The automorphism $b \mapsto b^x\,(b \in B)$ therefore has finite order, e say. Then x^e lies in the centre of A, so $C = \langle x^e \rangle \lhd A$. Also

$$|A:C| = |A:BC| \cdot |BC:C| \leq e|B| < \infty.$$

Proof of Proposition 2 Suppose the group G has a finite series (1) with each factor G_i/G_{i-1} either finite or cyclic; we are to show that G has a normal poly-C_∞ subgroup K of finite index. If $n = 1$, there is nothing to prove. If $n > 1$ we argue by induction. Thus we assume inductively that G_{n-1} has a normal poly-C_∞ subgroup L of finite index. By Lemma 2, with L for K and G_{n-1} for H, there exists $L^0 \lhd_f G_{n-1}$ with $L^0 \leq L$ and $L^0 \lhd G$. We now distinguish two cases.
Case 1 G/G_{n-1} finite. Then $L^0 \lhd_f G$, and we take $K = L^0$; (why is L^0 poly-C_∞? See Exercise 2 below!).
Case 2 $G/G_{n-1} \cong C_\infty$. Now apply Lemma 3, with G/L^0 for A and G_{n-1}/L^0 for B. This shows that there exists $K/L^0 \lhd_f G/L^0$ with $K/L^0 \cong C_\infty$. Since L^0 is poly-C_∞, K is also poly-C_∞ and the proof is finished.

Exercise 2 Suppose $\mathscr{P}$ is a property of groups such that every subgroup of a group with $\mathscr{P}$ also has $\mathscr{P}$. Show that every subgroup of a poly-$\mathscr{P}$ group is again poly-$\mathscr{P}$.

Before moving on to soluble groups in general, a fact about abelian groups:

Lemma 4 An abelian group is polycyclic if and only if it is finitely generated.

Proof ‘Only if’ is clear. Suppose conversely that $A = \langle a_1, \ldots, a_n \rangle$ is abelian. Then

$$1 \leq \langle a_1 \rangle \leq \langle a_1, a_2 \rangle \leq \ldots \leq \langle a_1, \ldots, a_{n-1} \rangle \leq \langle a_1, \ldots, a_n \rangle = A$$

is a series with cyclic factors, showing A to be polycyclic.

A group is called *soluble* if it is poly-abelian.

Definition For a group G, the *derived group* G' of G is the subgroup generated by all *commutators*

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

with $x, y \in G$;

$$G' = \langle [x, y] \mid x, y \in G \rangle = [G, G].$$

For $n > 1$, define

$$G^{(n)} = (G^{(n-1)})',$$

where $G^{(0)} = G$, $G^{(1)} = G'$.

Evidently, for any group G the *derived series*

$$G \geq G' \geq G^{(2)} \geq \ldots \geq G^{(n)} \geq G^{(n+1)} \geq \ldots$$

is a descending series of characteristic subgroups of G. The derived group G' is characterised by the properties

G/G' is abelian, and

if $N \triangleleft G$ and G/N is abelian, then $N \geqq G'$.

Proposition 3 Let G be a group.

(i) If G is soluble and $H \leq G$, then H is soluble.
(ii) If $N \triangleleft G$, then G is soluble if and only if both N and G/N are.
(iii) G is soluble if and only if $G^{(n)} = 1$ for some positive integer n.

Proof Exercise.

The least n for which $G^{(n)} = 1$ is called the *derived length* of the soluble group G.

Proposition 4 A soluble group has *max* if and only if it is polycyclic.

Proof 'If' we already know, and 'only if' follows from Lemma 4.

In contrast to Lemma 4, not every finitely generated soluble group has *max*. Let us construct a counterexample. Take

$$A = \underset{i=-\infty}{\overset{\infty}{\mathrm{Dr}}} \langle a_i \rangle$$

to be the restricted direct product of infinitely many infinite cyclic groups, and let x be the automorphism of A defined by

$$a_i^x = a_{i+1} \quad (-\infty < i < \infty).$$

Then x has infinite order and generates a group $\langle x\rangle \cong C_\infty$ of automorphisms of A. Now form the semi-direct product

$$G = A]\langle x\rangle.$$

Then G is soluble, and G is generated by two elements, namely a_0 and x. But the series

$$1 < \langle a_0\rangle < \langle a_0, a_1\rangle < \ldots < \langle a_0, a_1, \ldots, a_n\rangle < \ldots$$

shows that G does *not* have *max*. This group illustrates two constructions of wide usefulness: written additively, A becomes an $\langle x\rangle$-module, and as such it is isomorphic to the *group ring* $\mathbb{Z}\langle x\rangle$; and G itself is a so-called *wreath product*,

$$G = \langle a_0\rangle \wr \langle x\rangle \cong C_\infty \wr C_\infty.$$

B. Nilpotency

We move on now to discuss *nilpotency*, a concept which will be of central importance throughout.

Definition The *centre* of a group G is

$$\zeta_1(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

Evidently $\zeta_1(G)$ is a characteristic abelian subgroup of G. An element of G is called *central* if it lies in $\zeta_1(G)$. Now set $\zeta_0(G) = 1$ and define recursively

$$\zeta_i(G)/\zeta_{i-1}(G) = \zeta_1(G/\zeta_{i-1}(G)) \text{ for } i \geq 1.$$

Thus we obtain the *upper central series*

$$1 = \zeta_0(G) \leq \zeta_1(G) \leq \ldots \leq \zeta_n(G) \leq \zeta_{n+1}(G) \leq \ldots,$$

an ascending series of characteristic subgroups of G. It follows from the definition that for $n \geq 1$ and $x \in G$,

$$x \in \zeta_n(G) \Leftrightarrow [x, g] \in \zeta_{n-1}(G) \quad \forall g \in G.$$

More generally, a series of subgroups

$$1 = H_0 \leq H_1 \leq \ldots \leq H_k = G \tag{2}$$

is called a *central series* of G if for every $n \in \{1, \ldots, k\}$,

$$x \in H_n \Rightarrow [x, g] \in H_{n-1} \quad \forall g \in G.$$

Proposition 5 The following are equivalent:

(*a*) the series (2) is a central series of G;
(*b*) $H_n \lhd G$ for $1 \leq n \leq k$, and $H_n/H_{n-1} \leq \zeta_1(G/H_{n-1})$ for $1 \leq n \leq k$;
(*c*) $H_n \lhd G$ for $1 \leq n \leq k$ and for each n, the action of G by conjugation on the factor H_n/H_{n-1} is trivial.

The proof is immediate. We call a group G *nilpotent* if G has a (finite) central series.

Dual to the upper central series, one defines the *lower central series* of a group G,

$$G=\gamma_1(G)\geq\gamma_2(G)\geq\ldots\geq\gamma_n(G)\geq\gamma_{n+1}(G)\geq\ldots \tag{3}$$

by setting $\gamma_1(G)=G$ and for $n\geq 1$,

$$\gamma_{n+1}(G)=[\gamma_n(G),G]=\langle[x,g]\,|\,x\in\gamma_n(G),g\in G\rangle.$$

Then (3) is a descending central series of characteristic subgroups of G.

Proposition 6 Suppose (2) is a central series of G. Then $H_n\leq\zeta_n(G)$ and $H_{k-n}\geq\gamma_{n+1}(G)$ for $0\leq n\leq k$.

Proof Exercise.

An immediate consequence of Propositions 5 and 6 is now

Proposition 7 The following are equivalent for a group G:

(*a*) G is nilpotent;
(*b*) $\zeta_c(G)=G$ for some $c\in\mathbb{N}$;
(*c*) $\gamma_{c+1}(G)=1$ for some $c\in\mathbb{N}$.

If G is nilpotent, its *nilpotency class* is the length of a shortest central series of G (the length of the series (2) being the number k, i.e. the number of 'gaps'). It is now an easy exercise to improve Proposition 7 to:

$$G \text{ is nilpotent of class } \leq c\Leftrightarrow\zeta_c(G)=G\Leftrightarrow\gamma_{c+1}(G)=1.$$

Proposition 8 Subgroups and quotient groups of a nilpotent group are nilpotent. A direct product of finitely many nilpotent groups is nilpotent.

Exercise 3 Verify the above proposition. Construct counter-examples to disprove the following statements: (i) '$N\lhd G$, N nilpotent and G/N nilpotent $\Rightarrow G$ nilpotent'; (ii) 'a direct product of infinitely many nilpotent groups is nilpotent'.

Exercise 4 Let G be a group and $N\neq 1$ a normal subgroup of G. (i) Show that if G is nilpotent then $N\cap\zeta_1(G)\neq 1$. (ii) Show that if G is soluble then G has an abelian normal subgroup A with $1\neq A\leq N$. (iii) If G is

nilpotent and N is maximal among all abelian normal subgroups of G, then $C_G(N) = N$. (iv) If G is nilpotent then every subgroup of G is *subnormal*, i.e. if $H \leq G$ then there is a series $H = H_0 \lhd H_1 \lhd \ldots \lhd H_k = G$.
(*Hint*: (i) Consider the least j for which $N \cap \zeta_j(G) \neq 1$. (ii) Consider the derived series of N. (iii) If $C_G(N) > N$, consider the subgroup $N\langle x \rangle$ of G, where $xN \in \zeta_1(G/N) \cap C_G(N)/N$. (iv) Try $H_i = H\zeta_i(G)$.)

Nilpotent groups form a class intermediate between abelian groups and soluble groups. Let us consider some examples.

(1) *Finite p-groups* (The letter p denotes a prime number, and a finite p-group is a group whose order is a power of p.) If $G \neq 1$ is a finite p-group then $\zeta_1(G) \neq 1$, and $G/\zeta_1(G)$ is again a p-group, of smaller order than G. Therefore $\zeta_c(G) = G$ for some c and so G is nilpotent. For this, and the following result, see any book on finite group theory:

Theorem A finite group is nilpotent if and only if it is a direct product of p-groups (for various primes p).

(2) Let k be a field and n a positive integer. Denote by

$$\mathrm{Tr}_1(n, k)$$

the group consisting of all upper-triangular $n \times n$ matrices over k with all diagonal entries equal to 1; this is the *upper unitriangular group* of degree n over k. The group $\mathrm{Tr}_1(n, k)$ is nilpotent of class $n-1$, as we shall see later.

The last example is generalised in

Proposition 9 Let E be a ring (with 1) and I an ideal of E with $I^n = 0$. Put

$$G = 1 + I = \{1 + x | x \in I\} \subseteq E.$$

(i) G is a subgroup of the group of units of E.

(ii) Put $G_i = 1 + I^i$ for $i = 1, \ldots, n$; then

$$1 = G_n \leq G_{n-1} \leq \ldots \leq G_1 = G$$

is a central series of G, so G is nilpotent of class at most $n-1$.

(iii) For each $i < n$, the factor group G_i/G_{i+1} is isomorphic to the additive group of I^i/I^{i+1}.

(As usual, I^i denotes the ideal consisting of all finite sums $\sum x_1 x_2 \ldots x_i$ with each $x_j \in I$.)

Proof (i) For $x \in i$ we have

$$(1 + x)(1 - x + x^2 - \ldots \pm x^{n-1}) = 1$$

so each element of G is a unit in E; and

$$(1+x)(1+y) = 1 + (x + y + xy)$$

so G is closed under multiplication.

(ii) Note that each G_i is a subgroup of G, by the argument of part (i). If $g \in G_i$ and $h \in G$ then $g = 1 + x$, $h = 1 + y$ with $x \in I^i$ and $y \in I$. Now

$$gh - hg = xy - yx \in I^{i+1}$$

so $$[g,h] - 1 = g^{-1}h^{-1}(gh - hg) \in I^{i+1}$$

and so $[g,h] \in 1 + I^{i+1} = G_{i+1}$.

(iii) Define a map $\theta: G_i \to I^i/I^{i+1}$ by

$$g\theta = (g-1) + I^{i+1}.$$

Then for g and $h \in G_i$,

$$\begin{aligned}(gh)\theta &= (gh-1) + I^{i+1}\\ &= (g-1) + (h-1) + (g-1)(h-1) + I^{i+1}\\ &= (g-1) + (h-1) + I^{i+1}\end{aligned}$$

since $g - 1 \in I^i$, $h - 1 \in I^i \subseteq I$. Thus θ is a homomorphism. It is evident that θ is surjective and that $\ker\theta = G_{i+1}$.

To see how this generalises the case of $\mathrm{Tr}_1(n,k)$, consider a commutative ring R (with 1), a free R-module $V = R \oplus \ldots \oplus R$ (n summands), and take

$$E = \mathrm{End}_R(V) = M_n(R).$$

Put

$$V_i = \underbrace{0 \oplus \ldots \oplus 0}_{\leftarrow n-i \rightarrow} \oplus \underbrace{R \oplus \ldots \oplus R}_{\leftarrow i \rightarrow} \le V$$

and take

$$I = \{\alpha \in E \mid V_i\alpha \subseteq V_{i-1} \quad \text{for } i = 1, \ldots, n\}.$$

Thus I consists of all matrices over R of the form

$$\begin{bmatrix} 0 & * & \cdots & * \\ 0 & & \ddots & \vdots \\ \vdots & \ddots & & * \\ 0 & \cdots & 0 & 0 \end{bmatrix}$$

and we write $I = \mathrm{Tr}_0(n,R)$. Clearly $I^n = 0$, so the proposition assures us that the group

$$G = 1 + I = \mathrm{Tr}_1(n,R)$$

is nilpotent.

Exercise 5 (i) Show that I^i consists exactly of all matrices of the form

$$\begin{array}{c} \overset{\longleftarrow\; i \;\longrightarrow}{} \quad \overset{\leftarrow n-i \rightarrow}{} \\ \left[\begin{array}{cccccccc} 0 & \cdot & \cdot & \cdot & 0 & * & \cdots & * \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & * & \vdots \\ \cdot & & \cdot & & & & 0 & * \\ \cdot & & & \cdot & & & \vdots & 0 \\ \cdot & & & & \cdot & & \vdots & \\ \cdot & & & & & & 0 & \\ 0 & \cdot & \cdot & \cdot & & & 0 & 0 \end{array}\right] \end{array} \begin{array}{l} \updownarrow n-i \\ \\ \updownarrow i \end{array}$$

(the non-trivial part is that every such matrix belongs to I^i; this is where we need the hypothesis that $1 \in R$). (ii) Deduce that $G_i/G_{i+1} \cong R^+ \oplus \ldots \oplus R^+$ with $n-i$ summands, where R^+ denotes the additive group of R and $G_i = 1 + I^i$. (iii) Show that $G_i = \zeta_{n-i}(G)$ for $i = 1,\ldots,n$, hence that G is nilpotent of class exactly $n-1$. (*Hint*: argue by induction on $n-i$. Observe that for $g, h \in G$, $g^{-1}h \in G_m \Leftrightarrow g - h \in I^m$; apply this with $h = \alpha^{-1} g \alpha$, where α is a matrix of the form

$$\alpha_{pq} = \delta_{pq} + \delta_{pk}\delta_{(k+1)q}.)$$

(iv) If R is a field, then G is torsion-free if char $R = 0$, and G has exponent dividing p^{n-1} if char $R = p \neq 0$.

In the situation we have been considering, the R-module V is also a G-module; its submodules V_i are G-submodules and the induced action of G on each factor V_i/V_{i-1} is *trivial*. It is both possible and useful to generalize this setup to the 'non-linear' case: so let V be a group and G a group acting by automorphisms on V, and suppose

$$1 = V_0 \leq V_1 \leq \ldots \leq V_n = V \tag{4}$$

is a series of G-invariant normal subgroups of V such that the induced action G on each factor V_i/V_{i-1} is trivial. Then (4) is called a G-*central* series of V, G is said to *stabilize* the series (4), and we say that G acts *nilpotently* on V. The special case where $V = G$ and the action is by conjugation is already familiar – G acts nilpotently on itself if and only if G is nilpotent.

Proposition 10 If a group G acts faithfully on a group V and stabilizes a series of normal subgroups in V of length n, then G is nilpotent of class at most $n-1$.

Proof Say G stabilizes the series (4) above. We argue by induction on n. If $n = 1$ then $G = 1$ is nilpotent of class 0 (i.e. $\gamma_1(G) = 1$). Suppose $n > 1$ and put

$$C = C_G(V/V_1) \cap C_G(V_{n-1}).$$

Now $G/C_G(V/V_1)$ acts faithfully on V/V_1 and $G/C_G(V_{n-1})$ acts faithfully on V_{n-1}; applying the inductive hypothesis to these groups we obtain that

$$\gamma_{n-1}(G/C_G(V/V_1)) = \gamma_{n-1}(G/C_G(V_{n-1})) = 1,$$

whence

$$\gamma_{n-1}(G) \leq C_G(V/V_1) \cap C_G(V_{n-1}) = C.$$

Thus it will suffice now to show that $[C, G] = 1$. Take $c \in C$, $g \in G$, and $v \in V$. Then

$$v^g = wv$$

for some $w \in V_{n-1}$; and $v^{-1}v^c \in V_1$, so $(v^{-1}v^c)^g = v^{-1}v^c$. Therefore

$$v^c = v(v^{-1}v^c)^g = w^{-1}v^{cg}$$

so

$$v^{cg} = wv^c = (wv)^c = v^{gc}$$

(note that $w = w^c$ since $w \in V_{n-1}$). As v was arbitrary and the action of G is faithful, we deduce that $cg = gc$. Thus $[c, g] = 1$ as required.

Let us list some corollaries.

Corollary 1 For every group H, and all i and j,
$[\gamma_i(H), \gamma_j(H)] \leq \gamma_{i+j}(H)$.

Proof Take

$$V = \gamma_i(H)/\gamma_{i+j}(H),\ G = H/C_H(V)$$

and let G act on V via conjugation. Then G acts faithfully on V and stabilizes the series of length j whose lth term is $\gamma_{i+j-l}(H)/\gamma_{i+j}(H)$. The proposition shows that G is nilpotent of class at most $j-1$, thus $\gamma_j(H) \leq C_H(V)$. But this means nothing other than $[\gamma_i(H), \gamma_j(H)] \leq \gamma_{i+j}(H)$.

Corollary 2 If H is a group with $\gamma_n(H) = 1$ then $H^{(d)} = 1$ where $d = 1 + [\log_2 n]$.

For repeated applications of Corollary 1 give $H^{(i)} \leq \gamma_{2^i}(H)$, $i = 1, 2, \ldots, d$.

Corollary 3 For every group H and every i,
$[\zeta_i(H), \gamma_i(H)] = 1$.

Proof Apply Proposition 10 to $G = H/C_H(\zeta_i(H))$ acting by conjugation on $V = \zeta_i(H)$.