Prelude

A reminder

We have done our best to make this book reasonably self-contained. The intention is that a reader with no specialist knowledge of group theory, topology, number theory or Lie algebra theory should follow the main thread of the argument without undue difficulty. (This is less true of the 'Interludes', which touch on various topics, and of Chapter 13, which depends on a certain amount of commutative algebra.)

However, there are a number of elementary facts and concepts which are frequently used and can reasonably be classed under the heading of 'non-specialist knowledge'. These (apart from any that we may have missed) are collected together here, for the convenience of the reader.

0.1 Commutators

G denotes a group, x, y, z elements of G, and A, B, C subgroups of G.

$$x^y = y^{-1}xy, \quad [x,y] = x^{-1}x^y, \quad [x_1,\dots,x_n] = [[x_1,\dots,x_{n-1}],x_n].$$

$$[A,B] = \langle [a,b] \mid a \in A, b \in B \rangle$$

where $\langle X \rangle$ denotes the subgroup of G generated by a subset X of G.

$$[A,B,C] = [[A,B],C].$$

0.1. $[xy,z] = [x,z]^y[y,z]$, $[x,yz] = [x,z][x,y]^z$.

These are verified by inspection. Repeated applications of 0.1 give the first two claims of:

0.2. *For a positive integer n,*
(i) $[x^n,y] = [x,y]^{x^{n-1}} \cdot [x,y]^{x^{n-2}} \dots [x,y]^x \cdot [x,y]$;

(ii) $[x, y^n] = [x, y] \cdot [x, y]^y \ldots [x, y]^{y^{n-1}}$;
(iii) $(xy)^n \equiv x^n y^n [y, x]^{n(n-1)/2} \pmod{\gamma_3(G)}$.

Part (iii) is easily proved by induction on n, using (i). It is the beginning of the *Hall–Petrescu formula*, proved in full in Appendix A.

0.3 'Three-subgroup lemma'. *If A, B and C are normal subgroups of G then*

$$[A, B, C] \leq [B, C, A][C, A, B].$$

Proof This follows from the Hall–Witt identity:

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

which is most quickly verified by putting $u = acb^a, v = bac^b, w = cba^c$ and noting that $[a, b^{-1}, c]^b = u^{-1}v$, etc.

0.2 Nilpotent groups

The terms of the *lower central series* of a group G are defined by $\gamma_1(G) = G$, $\gamma_{i+1}(G) = [\gamma_i(G), G]$ for $i \geq 1$. The group G is *nilpotent*, of class at most c, if $\gamma_{c+1}(G) = 1$. The centre of G is $\mathrm{Z}(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$.

G is a *finite p-group* (where p is a prime) if $|G| = p^n$ for some n.

0.4. *Let G be a finite group.*

(i) *G is nilpotent if and only if $\mathrm{Z}(G/N) > 1$ for every proper normal subgroup N of G.*

(ii) *If G is a p-group then G is nilpotent.*

(iii) *If G is a p-group then every maximal proper subgroup of G is normal and has index p in G.*

(iv) *If G is nilpotent and $1 < N \lhd G$ then $[N, G] < N$ and $N \cap Z(G) > 1$.*

(v) *If G is nilpotent and $1 < N \lhd G$ then some maximal proper subgroup of N is normal in G.*

(vi) *If G is nilpotent then so are every quotient and every subgroup of G.*

(vii) *If G is nilpotent then the elements of finite order in G form a subgroup.*

Proof (i) *'If':* induction on $|G|$. By hypothesis, $1 < \mathrm{Z}(G) = Z$, say. Inductively, $\gamma_m(G/Z) = 1$ for some m. Then $\gamma_{m+1}(G) = 1$.

'Only if': Suppose $\gamma_{i+1}(G) = 1$. For some k, we then have $\gamma_{k+1}(G) \leq N$, $\gamma_k(G) \not\leq N$. This implies $1 < \gamma_k(G)N/N \leq \mathrm{Z}(G/N)$.

(ii) By (i), it suffices to show that $\mathrm{Z}(G) \neq 1$. Let $h_1, \ldots, h_r$ represent the non-central conjugacy classes of G. Then $|G : \mathrm{C}_G(h_i)| = p^{e_i} > 1$ so

$$|\mathrm{Z}(G)| = |G| - \sum_{i=1}^{r} |G : \mathrm{C}_G(h_i)| \equiv 0 \pmod{p}.$$

Since $|\mathrm{Z}(G)| \geq 1$ it follows that $|\mathrm{Z}(G)| \geq p$.

(iii) Let M be a maximal proper subgroup of G. By (ii), $\mathrm{Z}(G)$ contains an element z of order p. If $z \in M$, $M/\langle z \rangle$ is a maximal proper subgroup of $G/\langle z \rangle$ and we argue by induction. If $z \notin M$ then $M\langle z \rangle = G$. In this case $M \lhd G$ and $|G : M| = p$.

(iv) For some k, $\gamma_k(G) \cap N \neq 1$ and $\gamma_{k+1}(G) \cap N = 1$. Then $\gamma_k(G) \cap N \leq \mathrm{Z}(G) \cap N$, so $\mathrm{Z}(G) \cap N \neq 1$. If $[N, G] = 1$ then $[N, G] < N$. If $[N, G] > 1$, then (since $[N, G] \lhd G$) we have $1 < [N, G] \cap \mathrm{Z}(G) = K$, say. Then $1 < N/K \lhd G/K$ and we argue by induction.

(v) By (iv), $[N, G] < N$. Any maximal proper subgroup of N containing $[N, G]$ is necessarily normal in G.

(vi) Clear.

(vii) Let $x, y \in G$ have finite order; it will suffice to prove that the subgroup $H = \langle x, y \rangle$ that they generate is finite. Now $H/\gamma_2(H)$ is finite. Suppose that $\gamma_{i-1}(H)/\gamma_i(H)$ is finite for some $i \geq 2$. There is a well-defined bilinear mapping from $H/\gamma_2(H) \times \gamma_{i-1}(H)/\gamma_i(H)$ into $\gamma_i(H)/\gamma_{i+1}(H)$ given by

$$(a\gamma_2(H), b\gamma_i(H)) \mapsto [a, b]\gamma_{i+1}(H),$$

which induces an epimorphism $H/\gamma_2(H) \otimes \gamma_{i-1}(H)/\gamma_i(H) \to \gamma_i(H)/\gamma_{i+1}(H)$. Hence $\gamma_i(H)/\gamma_{i+1}(H)$ is finite. It follows by induction that $\gamma_i(H)/\gamma_{i+1}(H)$ is finite for every i; but $\gamma_{c+1}(H) = 1$ where c is the nilpotency class of G.

0.5. *Let G be any group and α an automorphism of G which induces the identity on $G/\gamma_2(G)$. Then α induces the identity on $\gamma_i(G)/\gamma_{i+1}(G)$ for every i.*

Proof There is an $\langle \alpha \rangle$-module epimorphism from

$$G/\gamma_2(G) \otimes \gamma_{i-1}(G)/\gamma_i(G)$$

onto $\gamma_i(G)/\gamma_{i+1}(G)$, given by

$$x\gamma_2(G) \otimes y\gamma_i(G) \mapsto [x,y]\gamma_{i+1}(G).$$

The result follows by induction on i.

0.3 Stability group theory

Suppose that H is a group acting faithfully by automorphisms on a group G.

0.6. If $N \lhd G$ and H induces the trivial action on both N and G/N, then H can be embedded in a Cartesian product of copies of $\mathrm{Z}(N)$.

Proof Let X be a set of generators for G. The embedding is given by the map $H \longrightarrow \prod_{x\in X} \mathrm{Z}(N)$,

$$h \mapsto (x^{-1}x^h)_{x\in X};$$

though not obvious, it is easily verified that $x^{-1}x^h$ does indeed lie in $\mathrm{Z}(N)$ for all $x \in G$.

If, in 0.6, the centre of N is torsion-free, or has a given finite exponent, etc., it follows that H has the same property.

0.7. *Let $G = G_0 \geq G_1 \geq \cdots \geq G_k = 1$ be a series of normal subgroups of G, and suppose that H fixes each G_i, and induces the trivial action on each factor G_i/G_{i+1}. Then*

(i) $\gamma_k(H) = 1$;

(ii) *if each G_i/G_{i+1} has exponent dividing m (respectively: is torsion-free), then H has exponent dividing m^{k-1} (respectively: is torsion-free).*

Proof Induction on k. Put $K = \mathrm{C}_H(G_1) \cap \mathrm{C}_H(G/G_{k-1})$. By the inductive hypothesis, $H/C_H(G_1)$ and $H/C_H(G/G_{k-1})$ satisfy (i) and (ii), with $k-1$ replacing k. Therefore so does H/K. Taking $a \in K$, $b \in H$ and $c \in G$ in the Hall–Witt identity $(*)$, we see that K is contained in the centre of H (apply $(*)$ to the semidirect product $G \rtimes H$). Therefore

$$\gamma_k(H) = [\gamma_{k-1}(H), H] \leq [K, H] = 1.$$

Also, 0.6 shows that in case (ii), K has exponent dividing m (respectively, K is torsion-free); hence (ii) follows.

Applying 0.7 to the conjugation action of G on $\gamma_i(G)$, we deduce that

$$[\gamma_i(G), \gamma_k(G)] \leq \gamma_{i+k}(G),$$

for any group G and all i and k (take $H = G/\mathrm{C}_G(\gamma_i(G)/\gamma_{i+k}(G))$ and replace G by $\gamma_i(G)/\gamma_{i+k}(G)$).

0.4 Unipotent groups

Let k be a finite field of characteristic p and $V = k^n$. The group $\mathrm{GL}_n(k)$ of all invertible $n \times n$ matrices over k may be identified with the group $\mathrm{GL}(V)$ of all k-linear automorphisms of V. We denote by $\mathrm{U}_n(k)$ the subgroup consisting of upper uni-triangular matrices. An automorphism g of V is *unipotent* if $(g-1)^n$ is the zero endomorphism. A *subgroup* H of $\mathrm{GL}_n(K)$ is said to be unipotent if each of its elements is unipotent.

0.8. *Let $H \leq \mathrm{GL}_n(k)$. The following are equivalent:*

(i) *H is unipotent.*

(ii) *The semidirect product $V \rtimes H$ is a nilpotent group.*

(iii) *There is a chain of H-invariant k-subspaces*

$$V = V_n > V_{n-1} > \cdots > V_1 > V_0 = 0$$

such that H induces the trivial action on each factor V_i/V_{i-1}.

(iv) *$(h_1 - 1)(h_2 - 1)\cdots(h_n - 1) = 0$ for all $h_1, \ldots, h_n \in H$.*

(v) *There exists $g \in \mathrm{GL}_n(k)$ such that $g^{-1}Hg \leq \mathrm{U}_n(k)$.*

(vi) *H is a finite p-group.*

Proof If h is unipotent then

$$h^{p^e} - 1 = (h-1)^{p^e} = 0$$

whenever $p^e \geq n$. Therefore (i) implies (vi). If H is a finite p-group then so is $V \rtimes H$, so (vi) implies (ii). It is easy to see that (ii)⇒(iii)⇒(iv)⇒(i) and that (iii)⇔(v).

0.5 Frattini subgroup

In this section, G denotes a finite p-group. The *Frattini subgroup* of G, denoted $\Phi(G)$, is the intersection of all maximal proper subgroups of G.

0.9. (i) $\Phi(G) = [G, G]G^p$.

(ii) *If $X \subseteq G$ and $X\Phi(G)$ generates $G/\Phi(G)$ then X generates G.*

(iii) $G/\Phi(G) \cong \mathbb{F}_p^d$ *where* d *is the minimal cardinality of any generating set for* G.

Proof (i) $G/[G,G]G^p$ is an elementary abelian p-group, so its maximal proper subgroups intersect in the identity. Therefore $\Phi(G) \leq [G,G]G^p$. The reverse inclusion follows from 0.4 (iii).

(ii) is clear, since if $\langle X \rangle < G$ then $\langle X \rangle \Phi(G)$ lies inside some maximal proper subgroup of G.

(iii) This now follows from (i) and (ii).

0.10. *Let* H *be the set of all automorphisms of* G *which induce the identity on* $G/\Phi(G)$. *Then* H *is a finite* p*-group.*

Proof It is enough to show that if $\alpha \in H$ has prime order q, then $q = p$. Let $\{x_1, \ldots, x_d\}$ be a generating set for G, and put

$$\Omega = \{(u_1 x_1, \ldots, u_d x_d) \mid u_1, \ldots, u_d \in \Phi(G)\},$$

a subset of $G \times \cdots \times G$ (with d factors). Then α permutes Ω, and has no fixed points, in view of 0.9 (ii). Therefore each orbit has length q and so $q \mid |\Omega| = |\Phi(G)|^d$. It follows that $q = p$.

0.6 Group algebras

Let G be a group and K a commutative ring. The group algebra of G over K, denoted $K[G]$, is defined to be the free K-module on the basis G, endowed with a product which extends simultaneously the group operation on G and the ring multiplication in K. Thus the elements of $K[G]$ are sums of the form $\sum_{g \in G} a_g g$, with each $a_g \in K$ and $a_g = 0$ for all but finitely many $g \in G$, and

$$(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{g \in G} c_g g$$

where

$$c_g = \sum_{x \in G} a_x b_{x^{-1}g}.$$

It is easily verified that $K[G]$ is a ring. One usually identifies K with the subring $K \cdot 1_G$ of $K[G]$, and G with the subgroup $1_K \cdot G$ of the group of units of $K[G]$. There is a homomorphism $\varepsilon : K[G] \to K$ given by

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g;$$

this is called the *augmentation*. Its kernel I is the *augmentation ideal* of $K[G]$; it is easy to see that

$$I = \{\sum a_g g \mid \sum a_g = 0\} = \sum_{g \in G \setminus 1} (g-1)K[G] = \bigoplus_{g \in G \setminus 1} K(g-1).$$

More generally, for any normal subgroup N of G there is a natural epimorphism $K[G] \to K[G/N]$, whose kernel is the right (or equivalently left) ideal generated by the set $\{g - 1 \mid g \in N\}$.

0.7 Topology

A topological space X is *Hausdorff* if distinct points of X have disjoint neighbourhoods; by a neighbourhood of x we mean any subset of X which contains an open set U with $x \in U$. A topological space X is *compact* if for any covering of X by open sets

$$X = \bigcup_{\alpha \in A} U_\alpha$$

there is a finite subset $\{\alpha_1, \ldots, \alpha_r\}$ of A such that

$$X = \bigcup_{i=1}^{r} U_{\alpha_i}.$$

0.11. *A space X is compact if and only if for each family $(Y_\alpha)_{\alpha \in A}$ of closed subsets of X with*

$$\bigcap_{\alpha \in A} Y_\alpha = \varnothing,$$

there exists a finite subset $\{\alpha_1, \ldots, \alpha_r\}$ of A such that

$$\bigcap_{i=1}^{r} Y_{\alpha_r} = \varnothing.$$

0.12. *If $f : X \longrightarrow Y$ is continuous and X is compact then $f(X)$ is compact.*

0.13.*Let X be a Hausdorff space.*

(i) *Every compact subspace of X is closed in X.*

(ii) *If X is compact, then every closed subset of X is compact (with the subspace topology).*

(iii) *If X is compact, then every infinite subset of X has a limit point in X.*

The proofs of 0.11–0.13 are simple exercises.

0.14. *If A and B are disjoint compact subsets of a Hausdorff space X, then there exist disjoint open subsets U and V of X with $A \subseteq U$ and $B \subseteq V$.*

Proof For each $a \in A$ and $b \in B$ there exist open sets $U(a,b)$, $V(a,b)$ with $a \in U(a,b)$, $b \in V(a,b)$ and $U(a,b) \cap V(a,b) = \varnothing$. Fix $a \in A$. Since B is compact, there exist $b_1, \ldots, b_r \in B$ such that $B \subseteq \bigcup_{i=1}^{r} V(a,b_i) = V(a)$, say. Put $U(a) = \bigcap_{i=1}^{r} U(a,b_i)$. Then the compactness of A gives $a_1, \ldots, a_s \in A$ such that $A \subseteq \bigcup_{i=1}^{s} U(a_j)$. Now let $U = \bigcup_{i=1}^{s} U(a_j)$, $V = \bigcap_{i=1}^{s} V(a_j)$.

0.15. *Let $f : X \longrightarrow Y$ be a continuous bijection, where X is compact and Y is Hausdorff. Then f is a homeomorphism.*

Proof We have to show that $f^{-1} : Y \longrightarrow X$ is continuous, i.e. that $(f^{-1})^{-1}(U)$ is open in Y for all U open in X. Now

$$(f^{-1})^{-1}(U) = f(U) = Y \setminus f(X \setminus U)$$

and $X \setminus U$ is compact. Therefore $f(X \setminus U)$ is compact, hence closed in Y, giving the result.

0.16. (Tychonoff's Theorem) *The product of any family of compact spaces is compact.*

For the proof see for example Higgins (1974), Chapter 1 (or any introductory topology textbook).

A *topological group* is a group G which is also a topological space, such that the maps

$$g \mapsto g^{-1} : G \to G$$
$$(g,h) \mapsto gh : G \times G \to G$$

are both continuous. Some less trivial results about topological groups are given in Appendix B; for most purposes, the following will suffice:

0.17. *Let G be a topological group.*

(i) *For each $g \in G$, the maps $x \mapsto xg$, $x \mapsto gx$, and $x \mapsto x^{-1}$ are homeomorphisms of G.*

(ii) *If H is a subgroup of G and H is open (respectively, closed), then every coset of H is open (respectively, closed).*

(iii) *Every open subgroup of G is closed.*

(iv) *G is Hausdorff if and only if $\{1\}$ is a closed subset of G.*

(v) *If N is a closed normal subgroup of G and G is Hausdorff, then G/N is Hausdorff (with the quotient topology).*

(vi) *If H is a subgroup of G and H contains a non-empty open subset U of G then H is open in G.*

Proof (i), (ii), (iii) are easy exercises. (iv): In a Hausdorff space, singleton subsets are closed (easy). Conversely, suppose $\{1\}$ is closed. Then every singleton is closed, by (i). Let $x \neq y$ be elements of G. Then $U = G \setminus \{xy^{-1}\}$ is open. Since the map $(a, b) \mapsto a^{-1}b$ is continuous, and $1 \in U$, there exist open neighbourhoods V_1 and V_2 of 1 such that $V_1^{-1} \cdot V_2 \subseteq U$. Then $V_1 x$ and $V_2 y$ are disjoint neighbourhoods of x, y. (v) follows from (iv). (vi): note that $H = \bigcup_{h \in H} Uh$.

0.8 Lie algebras

Let k be a commutative ring. A *Lie algebra* over k is a k-module L with a binary operation, (occasionally called the *Lie bracket*)

$$(\cdot, \cdot) : L \times L \to L$$

that is *k-bilinear* and satisfies

$$(a, a) = 0$$
$$((a, b), c) + ((b, c), a) + ((c, a), b) = 0$$

for all $a, b, c \in L$. The first condition implies

$$(a, b) = -(b, a)$$

for all a and b, and is equivalent to it unless 2 is a zero-divisor on L. The second condition is known as the *Jacobi identity*.

If A is any associative algebra over k, we may define a new binary operation on A, called *commutation*, as follows:

$$(a, b) = ab - ba.$$

It is easy to verify that with this operation A becomes a Lie algebra, the *commutation Lie algebra* on A.

A Lie algebra over $\mathbb{Z}$ is sometimes called a *Lie ring*.

Lie algebras over $\mathbb{R}$ appeared originally in the guise of 'infinitesimal Lie groups'; that is, as a sort of linearised approximation to a (real) Lie

group. As we shall see, Lie algebras over the p-adic numbers play the same role relative to p-adic Lie groups.

0.9 p-adic numbers

p will denote an arbitrary, but fixed, prime number. Each rational number $x \neq 0$ can be written uniquely as

$$x = p^n \cdot \frac{a}{b}$$

with $n, a, b \in \mathbb{Z}$, $b > 0$, $\gcd(a, b) = 1$ and $p \nmid ab$. We put

$$v_p(x) = n, \ |x|_p = p^{-n};$$

here $|\cdot|_p$ is the *p-adic absolute value* on $\mathbb{Q}$. This absolute value induces a metric on $\mathbb{Q}$, and the completion of $\mathbb{Q}$ with respect to this metric is *the p-adic field* $\mathbb{Q}_p$. Each element α of $\mathbb{Q}_p$ is thus the limit of a Cauchy sequence

$$\alpha = \lim_{i \to \infty} x_i$$

with $x_i \in \mathbb{Q}$ for each i, and the absolute value is extended to $\mathbb{Q}_p$ by setting

$$|\alpha|_p = \lim_{i \to \infty} |x_i|_p .$$

The 'valuation ring' in $\mathbb{Q}_p$ is the subring of *p-adic integers*

$$\mathbb{Z}_p = \left\{ \alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1 \right\}.$$

Each element of $\mathbb{Z}_p$ is the limit of a Cauchy sequence in $\mathbb{Q}$ whose terms all lie in $\mathbb{Z}$. It follows that each p-adic integer is the sum of a series

$$\sum_{n=0}^{\infty} a_n p^n \qquad (\dagger)$$

with each $a_n \in \mathbb{Z}$; moreover, each a_n may be chosen to lie in the set $\{0, 1, \ldots, p-1\}$, in which case the expression $(\dagger)$ is uniquely determined.

An alternative, equivalent, definition of $\mathbb{Z}_p$ is as the inverse limit of the system of rings

$$(\mathbb{Z}/p^n\mathbb{Z})_{n \in \mathbb{N}};$$

this construction is discussed in detail in Chapter 1.