Infinite groups 2016

January 12, 2017

0.1 Notation

$A \leq B$: A is a subgroup of B
$A \lhd B$: A is a normal subgroup of B
$x^y = y^{-1}xy$
elements a and b in a group G are *conjugate* if there exists $c \in G$ with $b = a^c$
$[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$; this is the *commutator* of x with y
$\langle Y \rangle$: subgroup generated by Y

1 Free groups

What is the 'most general' group generated by a given set? If G is a group and $Y \subseteq G$ then the subgroup $\langle Y \rangle$ *generated* by Y is the smallest subgroup of G that contains Y, namely the set of all products $y_1^{\pm 1} \dots y_n^{\pm 1}$ with $y_i \in Y$, $n \geq 0$. We say that Y generates G if $\langle Y \rangle = G$.

We say that Y *freely* generates G if the following additional property holds: any mapping $f : Y \to H$, for any group H, extends to a homomorphism $f^* : G \to H$. Note that f^* is unique, if it exists, because Y generates G.

In this case we also say: 'Y is a *basis* for G' and 'G is free on Y'. *A* group is *free* if it is free on some set.

If G is free on Y and G_1 is free on Y_1 then a bijection of sets $Y \to Y_1$ will extend to an isomorphism $G \to G_1$. So there is essentially at most one free group on Y.

Is there at least one?

X is a nonempty set, called an *alphabet*. $\overline{X} = \{\overline{x} \mid x \in X\}$ is a disjoint set bijective with X, and the inverse bijection $\overline{X} \to X$ is also denoted by $-$, so $\overline{(\overline{x})} = x$ for $x \in X$.

$W(X)$ denotes the set of *words* on this alphabet, i.e. expressions

$$w = y_1 \dots y_n$$

with each $y_i \in X \cup \overline{X}$. Here $n = l(w)$ is the length of w. Also $w = \varnothing \in W(X)$, with $l(\varnothing) = 0$. Words are multiplied by concatenation. $\varnothing$ acts as an identity for this product so it's usually denoted 1.

Words $w = uv$ and $w' = uy\overline{y}v$ where $y \in X \cup \overline{X}$ are *elementarily equivalent*. Two words w and w' are *equivalent* if one can be got from the other by a finite sequence of elementary equivalences: written $w \sim w'$.

The set of equivalence classes

$$F(X) := W(X)/\sim$$

is the *free group* on X. It's easy to see that $\sim$ respects multiplication, so $F(X)$ inherits the product from $W(X)$, and $F(X)$ is a group because

$$y_1 \dots y_n \cdot \overline{y_n} \dots \overline{y_1} \sim 1$$

(writing 1 also for the equivalence class of $\varnothing$).

A word w is *reducible* if $w = uy\overline{y}v$ where $y \in X \cup \overline{X}$. It is *reduced* otherwise. Obviously each equivalence class contains a reduced word.

Proposition 1.1 *Each equivalence class contains exactly one reduced word.*

Proof. Suffices to show that equivalent reduced words are equal. Let R denote the set of reduced words. For $x \in X \cup \overline{X}$ and $r \in R$ define $r\sigma(x)$ by

$$r\sigma(x) = rx \text{ if } rx \in R$$
$$r\sigma(x) = s \text{ if } r = s\overline{x}$$

(note that exactly one of these cases obtains). Thus $\sigma(x)$ maps R into R, and one checks quickly that $\sigma(x)\sigma(\overline{x})$ is the identity map on R, so $\sigma(x) \in \mathrm{Sym}(R)$ (the group of all permutations of R). Extend σ to a multiplicative map from $W(X)$ into $\mathrm{Sym}(R)$. Since $\sigma(x)\sigma(\overline{x}) = 1$ it follows that σ is constant on equivalence classes.

On the other hand, if w is reduced then $1\sigma(w) = w$. So if $w' \sim w$ and w' is also reduced then

$$w' = 1\sigma(w') = 1\sigma(w) = w.$$

■

Thus the elements of $F(X)$ are uniquely represented by the reduced words, and we often just identify $F(X)$ with the set of reduced words. Multiplication then goes like this: if w and w' are reduced, then the reduced word representing $ww\prime$ is obtained by *reducing* ww', i.e. deleting subwords of the form $y\overline{y}$, $y \in X \cup \overline{X}$, until none remain. The point of the Proposition is that it makes no difference in what order this process is done (which seems obvious but isn't, really!)

We usually identify X with its image in $F(X)$ ($x \in X$ is the unique reduced word in its equivalence class), and a word $w(X)$ with the element of $F(X)$ that it represents. But one needs to be a bit careful, since distinct words can represent the same element (unless they are both reduced). Thus $u = v$ can mean *either* 'u and v are identical words' *or* 'u and v represent the same element of $F(X)$'. If this distinction is relevant in an argument (which it often is!), one should

write $u \equiv v$ in the first case and $u =_F v$ in the second. To make matters worse, it is usual to write x^{-1} in place of $\overline{x}$. The main thing is to be clear about the distinction between a *word* and its *value* in a (free, or arbitrary) group.

With this convention in mind, we can state

Proposition 1.2 *$F(X)$ is free on X.*

Proof. Let $f : X \to H$ be a mapping, H being any group. Extend f to a mapping $f' : W(X) \to H$ by multiplicativity. Then f' is constant on equivalence classes so induces a map $f^* : F(X) \to H$. Clearly f^* is a homomorphism because f' is multiplicative, and for $x \in X$ we have $f^*(x) = f'(x) = f(x)$. ■

Thus: up to isomorphism there is exactly one group that is free on a set of given cardinality n; such a group is denoted F_n and is called 'the free group of rank n'.

Some basic facts (Ex. sheet 1).

Proposition 1.3 *$F_n \cong F_m$ if and only if $n = m$ (these can be any cardinal, not necessarily finite).*

Proposition 1.4 *Every free group is torsion-free, i.e. has no non-identity elements of finite order.*

Proposition 1.5 *Suppose that $\theta : G \to F$ is an epimorphism, where G is a group and F is a free group. Then there exists a monomorphism $\phi : F \to G$ such that $\theta \circ \phi$ is the identity map on F.*

Corollary 1.6 *If $N \lhd G$ and G/N is free then N has a free complement in G, i.e. G has a free subgroup H such that $NH = G$ and $N \cap H = 1$.*

Traditionally, free groups have been studied by *combinatorial* methods: algebra with words, and by *geometric* methods: groups acting on graphs. The latter provides a beautiful characterization:

Theorem 1.7 *A group is free if and only if it acts freely on a tree.*

The usefulness of this characterization is illustrated by its immediate corollary, the 'Nielsen-Schreier Theorem':

Theorem 1.8 *Every subgroup of a free group is free.*

Definitions:

A (directed) *graph* $\Gamma = (V, E)$ consists of a nonempty set $V = V(\Gamma)$ of 'vertices' and a set $E = E(\Gamma)$ of (directed) 'edges', and two maps $o, t : E \to V$. We picture vertices as points and edges as line segments; $o(e)$ is the *origin* of e and $t(e)$ is the *terminus* of e.

We assume that for each edge e there is an 'inverse' edge $\overline{e}$ with $o(\overline{e}) = t(e)$ and $t(\overline{e}) = o(e)$, and that $\overline{e} \neq e$ and that $\overline{\overline{e}} = e$. The pair $\{e, \overline{e}\}$ is called a 'geometric edge'.

A *path* from u to v ($u,\ v \in V$) is a sequence of edges $(e_1, \ldots, e_n)$ such that $o(e_1) = u,\ t(e_n) = v$ and $t(e_i) = o(e_{i+1})$ for $i = 1, \ldots, n-1$. Here $n \geq 1$ is the *length* of the path (so my convention is that a path is non-empty). The path is *reduced* if $e_{i+1} \neq \overline{e_i}$ for $i = 1, \ldots, n-1$ (this is often called a 'path without backtracking').

For a path $P = (e_1, \ldots, e_n)$ from u to v we write $\overline{P} = (\overline{e_n}, \ldots, \overline{e_1})$, the inverse path from v to u.

A *circuit* is a reduced path from u to u for some $u \in V$.

The graph Γ is *connected* if there is a path from u to v for every pair of distinct vertices u and v.

Γ is a *tree* if it is connected and has no circuits. Equivalently, provided $|V(\Gamma)| > 1$: for any $u \neq v \in V(\Gamma)$ there is a unique path from u to v. The length of this path is the *distance* from u to v.

A group G *acts* on Γ if G acts by permutations on both V and E, and preserves 'incidence': i.e.

$$\begin{aligned} o(ge) &= g(o(e)) \\ t(ge) &= g(t(e)) \\ g\overline{e} &= \overline{ge} \end{aligned}$$

for each $e \in E$ and $g \in G$.

We say that G acts *freely* if, in addition, every element of $G \smallsetminus \{1\}$ moves every vertex and every geometric edge: i.e. if $1 \neq g \in G$ then $gv \neq v$ for all $v \in V$ and $ge \notin \{e,\ \overline{e}\}$ for every $e \in E$.

The Cayley graph of a free group

Let G be a group and Y a subset of G. Define a graph $\Gamma = \mathcal{C}(G; Y)$ as follows:

$$\begin{aligned} V(\Gamma) &= G, \\ E(\Gamma) &= E_+ \dot{\cup} E_- \text{ where } E_+ = G \times Y,\ E_- = \overline{E_+} \\ o(g, y) &= g,\ t(g, y) = gy. \end{aligned}$$

This is called the *Cayley graph* of G w.r.t. Y.

G acts on Γ by left multiplication: hg (action) $= hg$ (group product), $h(g, y) = (hg,\ y)$, $h\overline{e} = \overline{he}$.

Proposition 1.9 *G acts freely on $\mathcal{C}(G; Y)$.*

Proof. If $hg = g$ then $h = 1$. If $he \in \{e,\ \overline{e}\}$ where $e = (g, y)$ then $he = e$ since $E_+ \cap E_- = \varnothing$; so $hg = g$ and $h = 1$. ■

Proposition 1.10 *G is freely generated by Y if and only if $\mathcal{C}(G;Y)$ is a tree.*

This implies the 'only if' part of Theorem 1.7.

Proof. Put $\Gamma = \mathcal{C}(G;Y)$ and write $S = Y \cup Y^{-1}$.

Suppose Y is a basis for G. Then $Y \cap Y^{-1} = \varnothing$, and for each edge $e = (g, y) \in E_+$ we will denote $\overline{e}$ by (gy, y^{-1}).

Let $u \neq v \in G$. Then $u^{-1}v = s_1 \dots s_n$ with $s_1, \dots, s_n \in S$ and $n \geq 1$. Put $e_1 = (u, s_1)$, $e_i = (us_1 \dots s_{i-1}, s_i)$ for $2 \leq i \leq n$. Then $(e_1, \dots, e_n)$ is a path from u to v. So Γ is connected.

Suppose that $P = (e_1, \dots, e_n)$ is a circuit in Γ. Now $o(e_1) = t(e_n) = u$, say, and there exist $s_j \in S$ such that $e_1 = (u, s_1)$, $e_i = (us_1 \dots s_{i-1}, s_i)$ for $2 \leq i \leq n$. Then $us_1 \dots s_n = u$ so $s_1 \dots s_n = 1$. Thus $s_1 \dots s_n$ is not reduced as a word on Y, and so $s_i s_{i+1} = 1$ for some $i < n$. But then

$$e_{i+1} = (us_1 \dots s_i, s_{i+1}) = (us_1 \dots s_i, s_i^{-1}) = \overline{e_i},$$

so p is not reduced. Thus Γ has no circuits, so Γ is a tree.

Assume now that Γ is a tree. Then again $Y \cap Y^{-1} = \varnothing$, for if $y, z \in Y$ then $((1, y), (y, z))$ is not a circuit, so $yz \neq 1$. So we can keep the notation $(gy, y^{-1}) := \overline{(g, y)}$.

Suppose $1 \neq v \in G$. There is a reduced path $(e_1, \dots, e_n)$ from 1 to v, and elements $s_i \in S$ such that $e_1 = (1, s_1)$, $e_i = (s_1 \dots s_{i-1}, s_i)$ for $2 \leq i \leq n$. Then $v = t(e_n) = s_1 \dots s_n$. Thus Y generates G.

Similarly, if $s_1 \dots s_n$ is reduced as a word on Y and $s_1 \dots s_n = 1$ in G then the corresponding path $(e_1, \dots, e_n)$ from 1 to $t(e_n) = 1$ is a circuit in Γ; but Γ has no circuits, so $s_1 \dots s_n$ is not equal to 1 in G. Thus Y freely generates G. ■

Groups acting on trees

To establish the other direction of Theorem 1.7, let T be a tree and suppose that G is a group acting freely on T. We need to find a basis for G. The way to do this is first to find a *fundamental domain* for the action.

Definition A *tree of representatives* for $G \setminus T$ is a subtree Δ of T such that each G-orbit in $V(T)$ contains exactly one vertex of Δ.

(A *subtree* means a subgraph that is a tree, and (U, E') is a *subgraph* of (V, E) if $U \subseteq V$, $E' \subseteq E$ and the maps $^{-}$, o, e restrict from E to E'.)

Lemma 1.11 *A tree of representatives exists.*

This is a special case of a general fact about graphs, which we'll prove below.

We first fix an *orientation* on T: a subset E_+ of $E(T)$ such that $E(T) = E_+ \dot{\cup} E_-$ where $E_- = \overline{E_+}$.

Now let $\Delta = (U, Z)$ be a tree of representatives for $G \setminus T$. Then $V(T)$ is the disjoint union of the subsets gU ($g \in G$). Let's say that gU is *adjacent* to

hU if $g \neq h$ (which is equivalent to gU and hU being disjoint) and there exists $e \in E_+$ with $o(e) \in hU$ and $t(e) \in gU$. In this case, there is exactly one such $e = e(h, g)$: if there were two we could construct a circuit passing through $g\Delta$ and $h\Delta$.

Let $Y = \{x \in G \mid xU \text{ is adjacent to } U\}$. Fix some $u \in U$.

Now form a new graph $\widehat{T}$ as follows. $V(\widehat{T}) = \{g\Delta \mid g \in G\}$, $E(\widehat{T}) = S_+ \dot{\cup} S_-$ where $S_+ = \{e(h, hy) \mid h \in G,\ y \in Y\}$,

$$o(e(h, hy)) = h\Delta$$
$$t(e(h, hy)) = hy\Delta.$$

Thus $\widehat{T}$ is obtained from T by collapsing each of the subtrees $g\Delta$ into a single vertex. Note that

$$E(T) = E(\widehat{T}) \overset{\bullet}{\cup} \bigcup_{c \in G} cZ.$$

It follows that $\widehat{T}$ is again a tree: given $g\Delta \neq h\Delta$ in $V(\widehat{T})$, there is a unique reduced path P in T from $hu \in h\Delta$ to $gu \in g\Delta$, and deleting from P the edges that lie in any cZ we obtain a path from $h\Delta$ to $g\Delta$; so $\widehat{T}$ is connected. Any circuit from $h\Delta$ to $h\Delta$ in $\widehat{T}$ can be expanded to a circuit in T from hu to hu by adding edges from $\bigcup_{c \in G} cZ$, because each of the subgraphs $c\Delta$ is connected; so $\widehat{T}$ has no circuits.

Now I claim that $\widehat{T}$ is isomorphic to $\mathcal{C}(G; Y)$. The mapping $g \longmapsto g^* := g\Delta$ is bijective, for if $g\Delta = h\Delta$ then $gu = hv$ for some $v \in U$ and then $h^{-1}gu = v \in U$, so $v = u$ as U contains just one representative of each G-orbit; but then $h^{-1}g = 1$ since G acts freely on T. Given $(h, y) \in G \times Y$, there is a unique $e = (h, y) \in E_+(\mathcal{C}(G; Y))$ with $o(e) = h$ and $t(e) = hy$; and there is a unique edge $e^* = e(h, hy) \in Z_+$ with $o(e^*) = h\Delta = h^*$ and $o(e^*) = hy\Delta = (hy)^*$. So the mapping $*$ is indeed a graph isomorphism.

It follows that $\mathcal{C}(G; Y)$ is a tree, and hence that Y freely generates G.

This completes the proof of Theorem 1.7.

It remains to prove

Lemma 1.12 *Let Γ be a connected graph and G a group acting on Γ. Then Γ has a connected subgraph Δ such that $V(\Delta)$ meets each G-orbit on $V(\Gamma)$ in exactly one point.*

Proof. Let's call a subgraph Δ of Γ *transversal* if each G-orbit in $V(\Gamma)$ contains at most one vertex of Δ. There exist connected transversal subgraphs, for example any subgraph with a single vertex and no edges. Order the set of all connected transversal subgraphs - let's call them CTs - by simultaneous inclusion of their vertex sets and their edge sets. Then it is clear that the union of an ascending chain of CTs is again a CT. Hence by Zorn's Lemma there exists a maximal CT $\Delta = (U, Z)$ say. It will suffice to show that U meets each orbit of G in $V(\Gamma)$.

If it doesn't, there exists $v \in V(\Gamma)$ such that $gv \notin U$ for all $g \in G$. Choose such a v so as to minimize the distance from Gv to U. Thus there exist $u \in U$ and $g \in G$, and a path $(e_1, \ldots, e_n)$ of length $n \geq 1$ from u to gv, and for no other choice of $v,\ u$ and g is there a shorter path. Say $t(e_1) = w$. Then $w \notin U$ (or we could replace u by w and reduce n), so $\Delta' = (U \cup \{w\}, Z \cup \{e_1, \overline{e_1}\})$ is a connected subgraph of T strictly bigger than Δ.

It follows that Δ' is not transversal, which implies that $hw \in U$ for some $h \in G$. But the distance from hw to hgv is $n-1$, which contradicts the definition of n. ■

Subgroups of a free group

Suppose that G is a subgroup of a free group F. Then F acts freely on a tree T, so G acts freely on T, so G is free. But we can do better: for the proof actually exhibits a basis for G. Of course, this depends on T. The natural choice is to take $T = \mathcal{C}(F, X)$ where F is free on X. Now choose a tree of representatives $\Delta = (U, Z)$ for the action of G on T. Then

$$\begin{aligned} F &= \bigcup_{g \in G} gU \text{ (disjoint union)} \\ &= \bigcup_{u \in U} Gu \text{ (disjoint union)}, \end{aligned}$$

so U is a transversal to the right cosets of G in F.

Now recall that $E(T) = E_+ \dot{\cup} \overline{E_+}$ where $E_+ = \{(h, x) \mid h \in F,\ x \in X\}$, with $o(h, x) = h$ and $t(h, x) = hx$. So for $g \in G$, gU is adjacent to U if and only if $g \neq 1$ and for some such h and x we have

$$h \in U,\ hx \in gU,$$

i.e. iff $g = vxu^{-1}$ for some $v,\ u \in U$. Thus G is freely generated by the set

$$Y = \left(UXU^{-1} \cap G\right) \smallsetminus \{1\}.$$

Given v and x we have $vx = gu$ for precisely one $g = g(v, x) \in G$ and one $u = u(v, x) \in U$; in fact $u(v, x)$ is the element of U representing the coset Gvx.

We may suppose that $1 \in U$. Since $U = V(\Delta)$ and Δ is a subtree of T, whenever $u \in U$ all the vertices along the path from 1 to u also belong to U; in terms of the free group $F(X)$ this means: *each initial segment of the reduced word representing u also belongs to U*. Such a transversal to the right cosets of G in F is called a 'Schreier transversal'. In fact this property characterizes the sets $V(\Delta)$ for Δ a tree of representatives. Thus we have

Corollary 1.13 *Let $G \leq F(X) = F$ and let U be a Schreier transversal to the right cosets of G in F. Then G is freely generated by the set*

$$\left(UXU^{-1} \cap G\right) \smallsetminus \{1\} = \left\{g(v, x) = vx \cdot u(v, x)^{-1} \mid v \in U,\ x \in X,\ vx \notin U\right\}.$$

Suppose now that $|U| = m$ and $|X| = d$ are finite. Let $\mathcal{E}$ denote the set of edges in E^+ having origin in U. Then $\mathcal{E} = E_+(\Delta) \cup \mathcal{F}$, disjoint union, where $E_+(\Delta) = E_+ \cap E(\Delta)$ and $\mathcal{F}$ is the set of edges e such that $o(e) \in U$ and $t(e) \in gU$ where gU is adjacent to U. Thus $|\mathcal{F}| = |Y|$.

Each vertex of T is the origin of d edges in E_+, so $|\mathcal{E}| = dm$. The tree Δ has m vertices, and therefore $|E_+(\Delta)| = m - 1$ (see next lemma). It follows that

$$|Y| = |\mathcal{F}| = |\mathcal{E}| - |E_+(\Delta)| = dm - (m-1) = 1 + m(d-1).$$

We have established *Schreier's formula*:

Theorem 1.14 *Let G be a subgroup of F_d of finite index $|F_d : G| = m$. Then G is free of rank $1 + m(d-1)$.*

We used the following (note that $E_+(\Delta)$ contains exactly one representative from each geometric edge $\{e, \overline{e}\}$):

Lemma 1.15 *Let Δ be a tree with $m < \infty$ vertices. Then Δ has $m-1$ geometric edges.*

Proof. We argue by induction on m. If $m = 1$ then Δ has no edges. Suppose that $m > 1$. Fix $u \in V(\Delta)$ and choose $v \in V(\Delta)$ at maximal distance from u. Let $(e_1, \ldots, e_n)$ be the path from u to v. Then e_n is the unique edge with $t(e_n) = v$; for if $v = t(e)$ for some edge $e \neq e_n$ then $(e_1, \ldots, e_n, \overline{e})$ is a path and $o(e)$ has distance $n+1$ from u.

It follows that if we remove e_n and $\overline{e_n}$ from $E(\Delta)$ and remove v from $V(\Delta)$ we are left with a subtree Δ_1. Now Δ_1 has $m-1$ vertices, so by inductive hypothesis it has $m-2$ geometric edges. Therefore Δ has $(m-2)+1 = m-1$ geometric edges. ■

2 Presentations

How does one define a particular group? If the group is finite, we can specify its multiplication table, but for an infinite group in general this is hopeless. One approach is to exploit the fact that every group is a homomorphic image of a free group. A free group is given by a generating set that satifies no relations. More generally, we can specify a group 'by generators and relations'.

Definition A *group presentation* is a pair $\mathcal{P} = (X; R)$ where X is a set, R is a set of words on X. The group presented by $\mathcal{P}$ is

$$\langle X; R \rangle := F(X) / \left\langle R^{F(X)} \right\rangle$$

where $\left\langle R^{F(X)} \right\rangle$ denotes the normal subgroup of $F(X)$ generated by R, that is, the subgroup generated by all conjugates of elements of R.

More generally, one writes $G = \langle X; R\rangle$ if the group G is generated by a subset X and the natural epimorphism π from $F(X)$ to G induces an isomorphism from $\langle X; R\rangle$ onto G, that is, if $\ker\pi$ is exactly $\left\langle R^{F(X)}\right\rangle$. In this case we say that $\mathcal{P}$ is a *presentation for* G, or that G is given by generators X and subject to the relations $R = 1$.

When X is given as a subset of G and w is a word on the alphabet X, $w(X)$ is also used to denote the evaluation of w in G; as mentioned above in the case of free groups, we have to be a little careful about which of the meanings for $w(X)$ is intended in any particular case. In case of possibe doubt, we say for example '$w = u$ in G'.to mean: w and u take the same value in G.

The following is clear from the universal property of $F(X)$:

Proposition 2.1 *Suppose that H is a group generated by a subset X^*, that $x \longmapsto x^*$ is a surjective mapping from X to X^*, and that $r(X^*) = 1$ for all $r \in R$. Then $*$ extends to an epimorphism from $G = \langle X; R\rangle$ onto H.*

Of course every group does have a presentation, for example the 'multiplication table representation': let $X = \{x_g \mid g \in G\}$ be a set bijective with G and let

$$R = \left\{x_g x_h x_{gh}^{-1} \mid g, h \in G\right\}.$$

Define $\pi : F = F(X) \to G$ by $\pi(x_g) = g$. Then $\left\langle R^{F(X)}\right\rangle \leq \ker\pi$. Since $F = \left\langle R^{F(X)}\right\rangle X$ it follows that $\ker\pi = \left\langle R^{F(X)}\right\rangle$, so $G = \langle X; R\rangle$.

Such a presentation can be unwieldy; when both X and R are finite sets, $\mathcal{P} = (X; R)$ is called a *finite presentation*. A group G is *finitely presented* (FP) if it has a finite presentation. Some groups are FP and some are not.

FP groups are among the most studied in mathematics; they arise naturally, for example, as fundamental groups of compact manifolds. A finite presentation is one way of specifying an infinite group with a finite amount of data.

A group specified in this way may be quite mysterious: this is the area of *decision problems*, discussed below. Still, the class of FP groups is quite well-behaved.

Theorem 2.2 *Let G be a group, $N \lhd G$ and $H \leq G$.*

i) *If both N and G/N are FP then G is FP.*

ii) *Suppose that $|G : H|$ is finite. Then G is FP if and only if H is FP.*

iii) *Suppose that G is finitely generated and that G/N is FP. Then $N = \left\langle Y^G\right\rangle$ for some finite subset Y.*

iv) *Suppose that G is FP and that $N = \left\langle Y^G\right\rangle$ for some finite subset Y. Then G/N is FP.*

Proof. (i) Say $N = \langle X; R\rangle$ and $G/N = \langle Y'; S\rangle$, where $X \subseteq N$ and $Y' \subseteq G/N$. For $y' \in Y'$ choose $y \in G$ so that $y' = Ny$. For $x \in X$ and $y \in Y$ we have $x^y = w_{x,y}(X)$, and for $s \in S$ we have $s(Y) = v_s(X)$ (where $s(Y)$ is the result of

substituting y for y' for each occurrence of a y' in s); here each $w_{x,y}$ and v_s is a word on the alphabet X.

Put

$$W = R \cup \left\{ x^{-y} w_{x,y}(X) \mid x \in X,\ y \in Y \right\} \cup \left\{ s(Y)^{-1} v_s(X) \mid s \in S \right\},$$

and set $\widetilde{G} = \langle X \cup Y; W \rangle$. Let $\widetilde{N} \leq \widetilde{G}$ be the subgroup generated by X. The middle set of relators in W ensures that $\widetilde{N} \lhd \widetilde{G}$, which implies that $\widetilde{G} = \widetilde{N} \langle Y \rangle = \langle X \rangle \langle Y \rangle$.

(To be absolutely clear we ought to use three different notations for X as a subset of G, as a subset of $\widetilde{G}$, and as an alphabet; but this requires a proliferation of x's, x^*s etc. and is more confusing than illuminating.)

Certainly $w(X, Y) = 1$ in G for each $w \in W$, so the identity map on $X \cup Y$ induces an epimorphism $\pi : \widetilde{G} \to G$. I claim that π is an isomorphism $\widetilde{G} \to G$, so $\langle X \cup Y; W \rangle$ is a presentation for G.

Suppose $v = g \cdot w(Y) \in \ker \pi$, with $g \in \widetilde{N}$. Then $w(Y) \in N$ so $w(Y') = 1$ in G/N, whence

$$w(Y') = \prod s_i(Y')^{\pm h_i}$$

in $F(Y')$ for some $s_i \in S$ and $h_i \in F(Y')$. Then in $\widetilde{G}$ we have

$$w(Y) = \prod v_{s_i}(X)^{\pm h_i^*} \in \widetilde{N}$$

for some $h_i^* \in \widetilde{G}$. Thus $v \in \widetilde{N} = \langle X \rangle$.

Say $v = u(X)$. Then the word $u(X)$ lies in the kernel of $F(X) \to N$, which is $\left\langle R^{F(X)} \right\rangle$; therefore $u(X) = 1$ in $\widetilde{G}$ since $R \subseteq W$. So $v = 1$. Thus π is injective as required.

(ii) Let $H \leq G$ with $|G : H|$ finite. Suppose that $G = \langle X; R \rangle$ with X and R finite. We have an epimorphism $\pi : F = F(X) \to G$ with $K = \ker \pi = \left\langle R^F \right\rangle$. Put $E = \pi^{-1}(H)$. Then $|F : E| = |G : H|$ is finite, so E is free on some finite basis Y. Since $K \leq E$, each $r \in R$ satisfies $r = s_r(Y)$ for some word s_r on Y. Put $S = \{ s_r(Y) \mid r \in R \}$. Then $\pi_1 = \pi_{|E} : E \to H$ is an epimorphism and

$$\ker \pi_1 = K = \left\langle S^F \right\rangle.$$

Say $F = a_1 E \cup \ldots \cup a_n E$. Then $S^F = (S^{a_1} \cup \ldots \cup S^{a_n})^E$. Thus $\langle Y; S^{a_1} \cup \ldots \cup S^{a_n} \rangle$ is a presentation for H.

Suppose conversely that H is FP. Let $N \leq H$ be a normal subgroup of finite index in G (Ex.sheet!). Then $|H : N|$ is finite, so N is FP by the first part. Also G/N is FP (Ex sheet). Therefore G is FP by (i).

****

Omitted: not examinable

(iii) We have an epimorphism $\pi : F(X) \to G/N$ with $\ker \pi = \left\langle R^{F(X)} \right\rangle$, where X and R are finite. For $x \in X$ choose $\widetilde{x} \in G$ such that $\pi(x) = N\widetilde{x}$. Then $\sim$ extends to a homomorphism from $F(X)$ into G, such that $G = N \left\langle \widetilde{X} \right\rangle$. As

G is finitely generated, there is a finite subset $\overline{U} \subseteq N$ such that $G = \left\langle \overline{U}, \widetilde{X} \right\rangle$ (write each generator as an element of N times a word on $\widetilde{X}$).

Let U be a set disjoint from X and bijective with $\overline{U}$ via $-$. Given any word $w(U, X) \in F(U, X)$, we have

$$w(U, X) = w_1(U^{F(X)}) \cdot w_2(X)$$

(move each occurrence of some u in w to the left, conjugating it by some word on X).

Claim:

$$N = \left\langle (\overline{U} \cup \widetilde{R})^G \right\rangle. \tag{1}$$

Certainly $(\overline{U} \cup \widetilde{R})^G \subseteq N$ since $N\widetilde{R}/N = \pi(R) = 1$. Suppose that $w(\overline{U}, \widetilde{X}) \in N$. Then $w_2(\widetilde{X}) \in N$. So

$$\pi(w_2(X)) = w_2(\widetilde{X})N = N \in G/N$$

and so $w_2(X) \in \ker \pi = \left\langle R^{F(X)} \right\rangle$.

Thus

$$w(\overline{U}, \widetilde{X}) = w_1(\overline{U}^{\langle \widetilde{X} \rangle}) \cdot w_2(\widetilde{X}) \in \left\langle \overline{U}^{\langle \widetilde{X} \rangle}, \widetilde{R}^{\langle \widetilde{X} \rangle} \right\rangle \subseteq \left\langle (\overline{U} \cup \widetilde{R})^G \right\rangle,$$

and (1) follows.

****

■

Proof. (iv) We have an epimorphism $\pi : F = F(X) \to G$ with $\ker \pi = \left\langle R^{F(X)} \right\rangle$, where X and R are finite.Suppose that $N = \left\langle Y^G \right\rangle$ for some finite subset Y of G. Say $y = \pi(w_y(X))$ for $y \in Y$, and put $W = \{w_y(X) \mid y \in Y\}$. Define $\pi_1 : F \to G/N$ by $\pi_1(w) = \pi(w)N$. Then $v \in \ker \pi_1$ if and only if

$$\begin{aligned} \pi(v) \in N &= \left\langle Y^G \right\rangle \\ &= \left\langle \pi(W)^{\pi(F)} \right\rangle \\ &= \pi \left\langle W^F \right\rangle, \end{aligned}$$

which holds if and only if

$$v \in \ker \pi \cdot \left\langle W^F \right\rangle = \left\langle R^F \right\rangle \left\langle W^F \right\rangle = \left\langle (R \cup W)^F \right\rangle.$$

Thus $\langle X; R \cup W \rangle$ is a presentation for G/N. ■

It is not always easy to tell if a given group is finitely presentable. Often arguments of a geometric or topological nature are used to find a finite presentation, when this exists. One approach to showing that a group is *not* FP uses part (iii) of the last theorem; this is illustrated in Ex sheet 2.

2.1 Decision problems

Historically these arose in topology: for example, given a space, is there an algorithm to determine whether a given loop can be shrunk to a point? In terms of the fundamental group, this asks: can one decide whether an arbitrary element of the group is equal to the identity? Of course this depends on how an element is supposed to be specified in the first place. Traditionally, one specifies the element as a word on a given generating set.

Let $\mathcal{P} = (X; R)$ be a finite presentation, and let $G = \langle X; R \rangle$ be a group presented by $\mathcal{P}$.

The *word problem (WP)* for $\mathcal{P}$ is *solvable* if there is an algorithm whose input is an arbitrary word w on X and whose output is YES if $w(X) = 1$ in G, NO if $w(X) \neq 1$ in G.

The *conjugacy problem (CP)* for $\mathcal{P}$ is *solvable* if there is an algorithm whose input is an arbitrary pair of words $u,\ v$ on X and whose output is YES if $u(X)$ and $v(X)$ are conjugate in G, NO if they are not.

Theorem 2.3 *Suppose that $G = \langle X; R \rangle = \langle Y; S \rangle$, both being finite presentations. Then WP (respectivly CP) is solvabe for $\langle X; R \rangle$ if and only if it is solvable for $\langle Y; S \rangle$.*

Thus it makes sense to say that the corresponding problem is or is not solvable for the group G. This theorem is not as simple to prove as some books suggest: the hard part is to find an algorithm that expresses each element of Y as a word in the generators X. In turn, this depends on the method of so-called *Tietze transformations*, which provides an algorithm that will effectively transform $\langle X; R \rangle$ into $\langle Y; S \rangle$, if these finite presentations represent isomorphic groups.

Theorem 2.4 (Novikov, Boone, et al) *There exist FP groups for which the word problem is not solvable. There exist FP groups for which the word problem is solvable but the conjugacy problem is not solvable.*

The proof of this fundamental result is beyond the scope of this course; it depends on recursive function theory, which is required to make precise the concept of 'algorithm'.

The third 'classical' decision problem is the *isomorphism problem*: is there an algorithm to decide whether two given finite presentations present isomorphic groups? This is also known to be unsolvable. Indeed, there is no algorithm to decide whether a given finite presentation presents the trivial group.

Thus it is a challenge to find a solution to any one of these problems in a particular group.

Theorem 2.5 *Both the word problem and the conjugacy problem are solvable for a finitely generated free group.*

Proof. We may assume that F is presented as $F = \langle X; \varnothing \rangle$. Given a word $w(X)$, let w^* be the reduced word obtained by deleting all subwords of the form xx^{-1} and $x^{-1}x$; this process certainly terminates since each deletion shortens the word. Then $w = 1$ in F if and only if w^* is the empty word. This solves the WP.

For CP see Ex sheet 1. ■

Definition A group G is *residually finite* if the normal subgroups of finite index in G intersect in 1.

Thus G is residually finite iff for each $g \in G \setminus \{1\}$ there exists $N \lhd G$ with G/N finite such that $g \notin N$.

Theorem 2.6 *Let G be a FP residually finite group. Then WP is solvable in G.*

Proof. Say $G = \langle X; R \rangle$. The algorithm consists of two procedures.

Procedure A: enumerate the consequences of '$R = 1$'. This means list all words of the form

$$u_1^{-1} r_1^{\pm 1} u_1 \cdot \ldots \cdot u_n^{-1} r_n^{\pm 1} u_n$$

where $u_1, \ldots, u_n$ are any words and $r_1, \ldots, r_n \in R$. Call the resulting list $(w_1, w_2, \ldots)$.

Procedure B: enumerate homomorphisms $\theta : G \to \mathrm{Sym}(n)$, $n \in \mathbb{N}$: these correspond to $|X|$-tuples of permutations that satisfy the relations $r = 1$, $r \in R$. Call the resulting list $(\theta_1, \theta_2, \ldots)$

Now let w be a word on X.

The nth step in the algorithm (a) compares w_n with w and (b) evaluates $\theta_n(w)$.

If $w = 1$ in G then w will appear as some w_n and the algorithm terminates with output YES.

If $w \neq 1$ in G then there exists $N \lhd G$ with G/N finite such that $w \notin N$. Say $|G/N| = m$ and let $\theta : G \to \mathrm{Sym}(m)$ be the permutation representation of G acting by right multiplication on the cosets of N. Then θ will appear as some θ_n in Procedure B, $\theta_n(w) = \theta(w) \neq 1$, and the algorithm terminates with output NO. ■

3 Soluble and nilpotent groups

Notation If a group G acts on a group V and $X \subseteq V$, $Y \subseteq G$

$$\begin{aligned} \mathrm{C}_G(X) &= \{g \in G \mid x^g = x \ \ \forall x \in X\} \\ \mathrm{C}_V(Y) &= \{v \in V \mid v^g = v \ \ \forall g \in Y\} \\ \mathrm{N}_G(X) &= \{g \in G \mid X^g = X\}. \end{aligned}$$

$\mathrm{C}_G(X)$ and $\mathrm{N}_G(X)$ are, respectively, the pointwise and setwise stabilizers of X, also called the *centralizer* and the *normalizer*, particularly when $V \lhd G$ and the action is conjugation.

Note that $\mathrm{C}_G(V)$ is exactly the kernel of the action of G on V, and hence that $G/\mathrm{C}_G(V)$ is isomorphic to a subgroup of $\mathrm{Aut}(V)$.

Since abelian groups are relatively easy to understand, it is useful to break up a group into abelian sections.

Definition let $A, B \leq G$. Then

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

G' is the *derived group* of G. Clearly G' is the smallest normal subgroup N such that G/N is abelian. Writing

$$\delta_0(G) = G$$
$$\delta_n(G) = \delta_{n-1}(G)'$$

we obtain the *derived series* $(\delta_n(G))$ of G, the fastest descending series of normal subgroups with abelian factors.

The group G is *soluble* if $\delta_n(G) = 1$ for some $n \geq 1$. Alternative notations: $\delta_2(G) = G''$, $\delta_n(G) = G^{(n)}$.

Lemma 3.1 *Let G be a group and $N \lhd G$. The following are equivalent:*

(a) *G has a chain of normal subgroups $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ such that G_i/G_{i-1} is abelian for each i;*

(b) *there exists a chain of subgroups $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ of G such that G_i/G_{i-1} is abelian for each i;*

(c) *both N and G/N are soluble;*

(d) *assuming in addition that G is* finite*: every composition factor of G is cyclic of prime order.*

If G is soluble, the *derived length* of G is the length of a shortest series of normal subgroups from 1 to G with abelian factors; equivalently it is the least n such that $\delta_n(G) = 1$.

Definition The *centre* of G is

$$\mathrm{Z}(G) = \mathrm{C}_G(G) = \{a \in G \mid [a,g] = 1\ \forall g \in G\}.$$

The *upper central series* is defined by

$$\mathrm{Z}_0(G) = 1$$
$$\mathrm{Z}_n(G)/\mathrm{Z}_{n-1}(G) = \mathrm{Z}(G/\mathrm{Z}_{n-1}(G)) \text{ for } n \geq 1,$$

equivalently: $\mathrm{Z}_n(G) = \mathrm{C}_G(G/\mathrm{Z}_{n-1}(G))$.

The *lower central series* is defined by

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

Note that $\gamma_2(G) = G' = \delta_1(G)$.

Thus (writing $Z_i = \mathrm{Z}_i(G)$ and $\gamma_i = \gamma_i(G)$) we have two series of normal subgroups

$$1 = Z_0 \leq Z_1 \leq \ldots \leq Z_n \ldots$$

and

$$G = \gamma_1 \geq \gamma_2 \geq \ldots \geq \gamma_n \ldots;$$

in fact they are *central series*: if $A \leq B$ are successive steps in such a series then $[B, G] \leq A$, equivalently $B/A \leq \mathrm{Z}(G/A)$.

The upper central series is the fastest ascending central series starting at 1, the lower central series is the fastest desecending central series starting at G.

A group G is *nilpotent* if G has a finite central series from 1 to G.

Lemma 3.2 *The following are equivalent: (a) G is nilpotent, (b) $\mathrm{Z}_n(G) = G$ for some finite n, (c) $\gamma_{n+1}(G) = 1$ for some finite n. If G is f*inite*, these are equivalent to (d) G is a direct product of p-groups.*

The least n satisfying (b) and the least n satisfying (c) are equal.

If G is nilpotent, the least n for which (b) or (c) holds is called the *nilpotency class* of G. (A finite group is a *p-group* if its order is a prime power p^k; the phrase 'p-group' is used a bit imprecisely to mean 'p-group for some prime p'.)

Obviously nilpotent groups are soluble, but not conversely (Ex sheet). If we want to prove something about soluble groups, we usually argue by induction on the derived length. Say G is soluble of derived length $n > 1$. Then the quotient G/G' is abelian and G' has derived length $n - 1$. Alternatively, the last non-trivial term $A = G^{(n-1)}$ of the derived series is abelian, and the quotient G/A has derived length $n - 1$.

If we want to construct examples of new soluble groups, a convenient approach is to start with a soluble group G and a G-module A, i.e. an abelian group A on which G is acting by automorphisms. Then consider the semi-direct product $A \rtimes G$.

Similarly, to prove something about nilpotent groups we often argue by induction on the class. To construct nilpotent groups, one usually looks for something with a nilpotent *action*, such as a triangular matrix group.

Proposition 3.3 *Let G be a group.* (i) $\delta_n(G) = 1$ *if and only if* $\delta_n(H) = 1$ *for every 2^n-generator subgroup H of G.*

(ii) $\gamma_n(G) = 1$ *if and only if* $\gamma_n(H) = 1$ *for every n-generator subgroup H of G.*

Proof. Define words δ_n and γ_n by

$$\delta_1(x, y) = \gamma_2(x, y) = [x, y],$$

$$\delta_{n+1}(x_1, \ldots, x_{2^{n+1}}) = [\delta_n(x_1, \ldots, x_{2^n}), \delta_n(x_{2^n+1}, \ldots, x_{2^n+2^n})]$$
$$\gamma_{n+1}(x_1, \ldots, x_{n+1}) = [\gamma_n(x_1, \ldots, x_n), x_{n+1}].$$

It is easy to see by induction on n that $\delta_n(G) = 1$ implies $\delta_n(x_1, \ldots, x_{2^n}) = 1$ and that $\gamma_n(G) = 1$ implies $\gamma_n(x_1, \ldots, x_n) = 1$ for all $x_1, x_2 \ldots \in G$. It will suffice to prove the converse. This is clear for δ_1 and for γ_2.

Suppose that $\delta_{n+1}(x_1, \ldots, x_{2^{n+1}}) = 1$ for all $\mathbf{x} \in G^{(2^{n+1})}$. Let $H = \left\langle \delta_n(x_1, \ldots, x_{2^n}) \mid \mathbf{y} \in G^{(2^n)} \right\rangle$. Then H is abelian, and normal in G. The word $\delta_n(x_1, \ldots, x_{2^n})$ takes only the value 1 in the quotient group G/H, so arguing by induction on n we may suppose that $\delta_n(G/H) = 1$. It follows that $\delta_{n+1}(G) = \delta_n(G)' \leq H' = 1$.

The argument for γ_n is similar, using 'central' in place of 'abelian'. ■

Remark The proof actually implies that $\delta_n(G)$, $\gamma_n(G)$ are so-called 'verbal subgroups', namely the subgroups generated by all values of the words δ_n, γ_n respectively (and this fact retrospectively justifies the choice of notation).

Group actions and 'stability groups'

$\mathrm{Aut}(G)$ denotes the group of automorphisms of of a group G. For $x \in \mathrm{Aut}(G)$, $g \in G$ we write g^x for the action of x on g, and $[g, x] = g^{-1}g^x$. This is consistent with the notation for conjugates and commutators if we think of G and $\mathrm{Aut}(G)$ as both embedded in the semi-direct product $G \rtimes \mathrm{Aut}(G) = \mathrm{Hol}(G)$ (the *holomorph* of G).

Notation

$$[x, y, z] = [[x, y], z]$$

To say that a group G *acts* on another group V means: to each $g \in G$ there is an automorphism α_g of V, such that $\alpha : G \to \mathrm{Aut}(V)$ is a homomorphism. One usually writes $v \longmapsto v^g$ for the action of α_g on $v \in V$.

Proposition 3.4 *The following hold in all groups.*

$$\begin{aligned} [x, y] &= [y, x]^{-1} \\ [xy, z] &= [x, z]^y [y, z] \\ [x, yz] &= [x, z][x, y]^z \\ [x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x &= 1. \end{aligned}$$

Proof. For the last line, put $u = xzx^{-1}yx$, $v = yxy^{-1}zy$, $w = zyz^{-1}xz$ and note that $u^{-1}v = [x, y^{-1}, z]^y$ etc. ■

Corollary 3.5 *Let $A, B, C \leq G$.* (i) If $A = \langle X \rangle$ *and* $B = \langle Y \rangle$ *and* $\langle A, B \rangle = H$ *then*

$$[A, B] = [B, A] = \left\langle [x, y]^h \mid x \in X,\ y \in Y,\ h \in H \right\rangle \lhd H.$$

(ii) $[A, G]A = A[A, G] = \left\langle A^G \right\rangle$.

(iii) 'Three-Subgroup Lemma' *If $N \lhd G$ then*

$$[[B, C], A] \leq N \text{ and } [[C, A], B] \leq N \Longrightarrow [[A, B], C] \leq N.$$

In particular, if $A, B, C \lhd G$ then

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

Proof. (i) Note first that $[A,B] = [B,A]$ because $[a,b] = [b,a]^{-1}$. If $a, c \in A$ and $b \in B$ then $[a,b]^c = [ac,b][c,b]^{-1} \in [A,B]$; therefore $A \leq \mathrm{N}_G([A,B])$. Similarly $B \leq \mathrm{N}_G([B,A]) = \mathrm{N}_G([A,B])$. Therefore $H = \langle A, B\rangle \leq \mathrm{N}_G([A,B])$, so $[A,B] = [B,A] \lhd H$.

Put $W = \left\langle [x,y]^h \mid x \in X,\ y \in Y,\ h \in H \right\rangle$. Then $W \lhd H$ and X and Y commute elementwise modulo W, so $[A,B] \leq W$. The reverse inclusion follows from $[A,B] \lhd H$.

(ii) Immediate from

$$a^g = a[a,g] = [a, g^{a^{-1}}]a.$$

(iii) By (i), $[[A,B],C]$ is generated by conjugates of elements $[a, b^{-1}, c]$ ($a \in A$, $b \in B$, $c \in C$). But

$$[a,b^{-1},c]^{-1} = [b,c^{-1},a]^{cb^{-1}}[c,a^{-1},b]^{ab^{-1}} \in N.$$

■

Proposition 3.6 *Suppose that $U \lhd V$ and that $G \leq \mathrm{Aut}(V)$ satisfies*

$$[U,G] = 1,\ [V,G] \leq U. \tag{2}$$

(i) *G is abelian.*

(ii) *For $v \in V$ define $\theta_v : G \to U$ by $\theta_v(g) = [v,g]$. If $V = U\langle T\rangle$ for some subset T then the mapping*

$$g \longmapsto (\theta_v(g))_{v \in T}$$

is an injective homomorphism from G into $\prod_{v\in T} \mathrm{Z}(U)$.

Proof. (i) In the group $\mathrm{Hol}(V)$ we have

$$[[V,G],G] = [[G,V],G] \leq [U,G] = 1.$$

Therefore $[[G,G],V] = 1$ by the Three-Subgroup Lemma. But $[[G,G],V] = [G',V] = [V,G']$ so $G' = 1$.

(ii) Here $\prod_{v\in T} \mathrm{Z}(U)$ means the Cartesian product of copies of $\mathrm{Z}(U)$ indexed by T. The proof is an *exercise* on sheet 3. ■

More generally, we have

Theorem 3.7 *Let $1 = V_0 \leq V_1 \leq \ldots \leq V_n = V$ be a series of normal subgroups of V. Suppose that $G \leq \mathrm{Aut}(V)$ satisfies*

$$[V_i, G] \leq V_{i-1}\ (1 \leq i \leq n).$$

Then $\gamma_n(G) = 1$.

Proof. Note that G maps each V_i to itself, and so G acts on both V_i and V/V_i.

If $n = 1$ the conclusion equals the hypothesis. (If $n = 2$ this is the preceding proposition, but the proof includes that case.) Suppose that $n > 1$ and argue by induction on n. Write $G_{n-1} = \gamma_{n-1}(G)$. The inductive hypothesis implies that $\gamma_{n-1}(G)$ acts trivially both on V/V_1 and on V_{n-1}, so

$$[V, G_{n-1}] \leq V_1,\ [V_{n-1}, G_{n-1}] = 1.$$

Therefore $[[V, G_{n-1}], G] = 1$ and $[[V, G], G_{n-1}] \leq [V_{n-1}, G_{n-1}] = 1$. Now the Three-Subgroup Lemma gives $[[G_{n-1}, G], V] = 1$. Thus $\gamma_n(G) = [G_{n-1}, G]$ acts trivially on V and so $\gamma_n(G) = 1$. ■

Typical applicaton: V is an n-dimensional vector space k^n and G is the group of upper uni-triangular matrices over the field k.

Nilpotent groups

If G is a nilpotent group, many of its properties are already determined by the pieces G/G' and $\mathrm{Z}(G)$. Here are some examples.

Theorem 3.8 ('Going up') *Let $Z_i = \mathrm{Z}_i(G)$, $i \geq 0$. Let $\mathcal{P}$ be the property 'torsion-free', or the property 'of exponent dividing m' for some $m \in \mathbb{N}$. If Z_1 has $\mathcal{P}$ then so does Z_i/Z_{i-1} for each $i \geq 1$.*

Proof. $Z_1/Z_{1-1} = Z_1$. Let $i > 1$ and suppose inductively that Z_{i-1}/Z_{i-2} has $\mathcal{P}$. Write $- : G \to G/Z_{i-2}$ for the quotient mapping.

Define $\sigma : G \to \mathrm{Aut}(G/Z_{i-2})$ by $\overline{h}^{\sigma(g)} = \overline{h^g}$. Now $\sigma(Z_i)$ acts trivially both on G/Z_{i-1} and on Z_{i-1}/Z_{i-2}; it follows by Proposition 3.6(ii) that $\sigma(Z_i)$ inherits $\mathcal{P}$ from Z_{i-1}/Z_{i-2}. But $\sigma(Z_i) \cong Z_i/Z_{i-1}$ since $\ker \sigma = Z_{i-1}$. ■

Corollary 3.9 *Let G be a nilpotent group, of nilpotency class c. If $\mathrm{Z}(G)$ is torsion-free then so is G. If $\mathrm{Z}(G)$ has exponent dividing m then G has exponent dividing m^c.*

Theorem 3.10 ('Going down') *Let $\Gamma_i = \gamma_i(G)$, $i \geq 1$. Let $\mathcal{P}$ be the property 'finitely generated', or the property 'of exponent dividing m' for some $m \in \mathbb{N}$, or the property 'periodic'. If G/G' has $\mathcal{P}$ then so does Γ_i/Γ_{i+1} for each i.*

Proof. Put $A_i = \Gamma_i/\Gamma_{i+1}$. Assume that A_1 has $\mathcal{P}$. Let $i \geq 1$ and suppose inductively that A_i has $\mathcal{P}$. The commutator mapping induces a bilinear map $\psi : A_i \times A_1 \to A_{i+1}$, and $\psi(A_i \times A_1)$ generates A_i (see Ex Sheet 3).

Let $a \in A_1$ and $b \in A_i$. If $a^m = 1$ then $\psi(b, a)^m = \psi(b, a^m) = 1$; so if A_1 has exponent dividing m then A_{i+1} is an abelian group generated by elements of order dividing m, and so A_{i+1} has exponent dividing m. Similarly, if A_1 is periodic then A_{i+1} is an abelian group generated by elements of finite order, and so A_{i+1} is periodic.

Now suppose that $A_1 = \langle X \rangle$ and $A_i = \langle Y \rangle$ where X and Y are finite sets. Then A_{i+1} is generated by the finite set $\psi(Y, X)$; for if $a = \sum_{x \in X} r_x x$ and $b = \sum_{y \in Y} s_y y$ ($r_x,\ s_y \in \mathbb{Z}$) (writing the group operation additively in these abelian groups) then

$$\psi(b, a) = \sum_{y,x} r_x s_y \psi(y, x).$$

■

Corollary 3.11 *Let G be a nilpotent group, of nilpotency class c. If G/G' is finitely generated then so is G. If G/G' has exponent dividing m then G has exponent dividing m^c. If G/G' is periodic then so is G. If G/G' is finite, then so is G.*

For a more direct proof of the first claim see Ex sheet 3.

Corollary 3.12 *Let G be a nilpotent group and let T denote the set of all elements of finite order in G. Then T is a normal subgroup of G and G/T is torsion-free.*

Proof. Let $a,\ b \in T$. We need to show that $a^{-1}b \in T$; the rest then follows easily. Put $H = \langle a, b \rangle$. Then H is nilpotent and H/H' is an abelian group generated by two elements of finite order, so H is finite. Therefore $a^{-1}b \in H \subseteq T$. ■

Corollary 3.13 *Let G be a nilpotent group. If G is finitely generated then every subgroup of G is finitely generated.*

Proof. If G is abelian this follows from the structure theory of f.g. abelian groups (= f.g. $\mathbb{Z}$-modules); it can also be proved very easily by induction on the number of generators, starting with the fact that every subgroup of a cyclic group is cyclic (exercise!)

In general, say G is nilpotent of class $c > 1$ and let $H \leq G$. Put $A = \gamma_c(G)$. Then A is a finitely generated abelian group by Theorem 3.10, so $H \cap A$ is f.g. by the abelian case. Also $H/(H \cap A) \cong AH/A \leq G/A$ and G/A is f.g. nilpotent of class $c - 1$, so arguing by induction we may suppose that $H/(H \cap A)$ is f.g.. It follows that H is f.g.. ■

Corollary 3.14 *Every finitely generated nilpotent group is finitely presented.*

Proof. Say $1 = \gamma_{c+1}(G) < \gamma_c(G) = A$ and G is finitely generated. Then A is a finitely generated abelian group, so A is FP. Also G/A has nilpotency class $c-1$, and arguing by inducton on c we may suppose that G/A is FP. Therefore G is FP. ■

Nilpotent normal subgroups

Lemma 3.15 (i) *If N is nilpotent and A is maximal among abelian normal subgroups of N then $\mathrm{C}_N(A) = A$.*

(ii) *Let G be a soluble group and B an abelian normal subgroup of G. Then G has a normal subgroup $N \geq B$ such that $\gamma_3(N) = 1$ and $\mathrm{C}_G(N) = \mathrm{Z}(N)$.*

This is often used to infer properties of G from properties of its abelian subgroups. Suppose, for example, that A in (i) is known to be finite. Then $N/A = N/\mathrm{C}_N(A)$ is isomorphic to a subgroup of $\mathrm{Aut}(A)$, and so N is finite. If N itself arises as in (ii), it follows similarly that $G/\mathrm{Z}(N) = G/\mathrm{C}_G(N)$ is finite, and hence that G is finite.

Proof. of Lemma 3.15. (i) Suppose that $C := \mathrm{C}_N(A) > A$. Put $W/A = \mathrm{Z}(N/A)$. Then $1 \neq C/A \lhd N/A$, so $(C \cap W)/A = C/A \cap W/A > 1$ (Ex. sheet 3). Let $w \in C \cap W \setminus A$ and put $B = A\langle w \rangle$. Then $A < B$. But $[w, N] \subseteq A$, so $B \lhd G$, and B is abelian: this contradicts the maximality of A.

(ii) Let A be maximal among abelian normal subgroups of G that contain B (such a thing exists by **Zorn's Lemma**). Then $A \leq C := \mathrm{C}_G(A)$.

Case 1: If $A = C$ take $N = A$.

Case 2: Suppose that $A < C$. Then G/A has an abelian normal subgroup N/A with $A < N \leq C$ (Ex. sheet 3). Choose N maximal such, and put $D = \mathrm{C}_G(N)$. Then

$$\gamma_3(N) = [N', N] \leq [A, C] = 1.$$

Now $A \leq D \leq C$. Suppose $A < D$. Then G/A has an abelian normal subgroup $X/A > 1$ with $X \leq D$. Then

$$[XN, XN] \leq X'[X, N]N' \leq A,$$

so XN/A is abelian. Since $XN \leq C$ this implies that $X \leq N$, so

$$X \leq N \cap D = \mathrm{Z}(N) = A$$

since $\mathrm{Z}(N)$ is an abelian normal subgroup of G containing A. Contradiction! ■

Finitely generated metabelian groups

We have seen that every finitely generated nilpotent group is finitely presented; so there are only countably many such groups up to isomorphism. On the other hand, an exercise on Sheet 2 shows how to construct uncountably many 2-generator soluble groups. So we can expect these in general to be much wilder. Here we'll look at some restricted classes of soluble groups that are not too complicated.

A group G is *metabelian* if it is soluble of derived length at most 2, i.e. if $G'' = 1$. In this case, the derived group $G' = A$ is abelian, and we can consider A as a module for $G/A = Q$. The action of Q on A is defined by

$$a^{\overline{g}} = a^g \ (a \in A, \ g \in G)$$

where $\overline{g} = Ag \in Q$. The *group ring* $\mathbb{Z}Q$ is the ring whose additive group is the free $\mathbb{Z}$-module on the basis Q, with multiplication extending the group multiplication on Q. Thus it consists of finite sums

$$\sum_{g \in G} n_g g$$

with $n_g \in \mathbb{Z}$, all but finitely many of them zero; and

$$\left(\sum_{x \in G} n_x x\right) \cdot \left(\sum_{y \in G} m_y y\right) = \sum_{g \in G} \left(\sum_{xy=g} n_x m_y\right) g.$$

Extending the action by linearity, any Q-module becomes a $\mathbb{Z}Q$-module.

Proposition 3.16 *Let G be a finitely generated metabelian group with derived group A, and set $Q = G/A$. Then $\mathbb{Z}Q$ is a finitely generated $\mathbb{Z}$-algebra and A is a finitely generated $\mathbb{Z}Q$-module.*

Proof. Say G is generated by a finite set X. Then Q is generated by $\overline{X}$ and then $\mathbb{Z}Q$ is generated by $\overline{X}$ as a $\mathbb{Z}$-algebra. Since G/A is a finitely generated abelian group, it is finitely presented; as G is finitely generated, it follows that A is finitely generated as a normal subgroup of G; this is the same as saying that it is finitely generated as a $\mathbb{Z}Q$-module. ■

Hilbert's Basis Theorem says that a finitely generated commutative rings are Noetherian; thus $\mathbb{Z}Q$ is a Noetherian ring and A is a Noetherian $\mathbb{Z}Q$-module. The analogous condition for groups is *max-n*, the ascending chain condition for normal subgroups: every strictly ascending chain of normal subgroups is finite.

Theorem 3.17 *Let G be a finitely generated metabelian group. Then every normal subgroup of G is finitely generated as a normal subgroup, and G satisfies* max-n.

Corollary 3.18 *There are only countably many f.g. metabelian groups up to isomorphism.*

Proof. Fix $d \in \mathbb{N}$ and put $F = F_d$. Every d-generator metabelian group is isomorphic to F/N where $F'' \leq N \lhd F$. By Applying the theorem to F/F'' we see that each such N is of the form $F'' \left\langle Y^F \right\rangle$ where $Y \subseteq F$ is finite. The number of such subsets Y is countable. ■

Proof. of Theorem 3.17. Let G, $A = G'$ and $Q = G/A$ be as above. Let $N \lhd G$. Then $N \cap A$ is a $\mathbb{Z}Q$-submodule of A, and as such is finitely generated, since A is a Noetherian $\mathbb{Z}Q$-module by HBT. Thus

$$N \cap A = \left\langle Y^Q \right\rangle = \left\langle Y^G \right\rangle$$

for some finite set $Y \subseteq N$. On the other hand, $N/(N \cap A) \cong NA/A$ is a subgroup of the f.g. abelian group G/A, so $N/(N \cap A)$ is finitely generated; say $N = (N \cap A)\langle X \rangle$ for some finite set $X \subseteq N$. It follows that $N = \langle X \cup Y^Q \rangle = \langle W^Q \rangle$ where $W = X \cup Y$.

Now let $N_1 \leq N_2 \leq \ldots \leq N_n \leq \ldots$ be an ascending chain of normal subgroups of G. Put $N = \bigcup_{i=1}^{\infty} N_i$. Then $N = \langle W^Q \rangle$ for some finite set $W \subseteq N$. Since W is finite there exists $k \in \mathbb{N}$ such that $W \subseteq N_k$, and it follows that $N_n = N_k$ for all $n \geq k$. Thus the infinite chain (N_i) is not strictly ascending. (Note that *any* strictly ascending chain must contain a strictly ascending subchain indexed by $\mathbb{N}$.) Thus G satisfies max-n. ■

Remark The condition max-n is equivalent to: 'every non-empty collection $\mathcal{S}$ of normal subgroups has a maximal member' ($N \in \mathcal{S}$ is *maximal* if $N \leq K \in \mathcal{S} \Longrightarrow N = K$.) This equivalence is a general feature of chain conditions, and should be checked as an *exercise* (see the 'Commutative Algebra' course).

****

OMITTED

For the next result we need to quote some deeper commutative algebra.

Theorem 3.19 *Let R be a finitely generated commutative $\mathbb{Z}$-algebra, M a simple R-module, and A a finitely generated R-module containing M such that $M \leq B$ for every submodule $B \neq 0$ of A. Then A is finite.*

Proof. Put $I = \mathrm{ann}_R(M)$. Then $R/I \cong M$ is a commutative ring that is simple as a module for itself, so it is a field. A version of the '*Weak Nullstellensatz*' asserts that a field which finitely generated as a $\mathbb{Z}$-algebra is finite. Therefore R/I is finite.

The *Artin-Rees Lemma* shows that $AI^n \cap M \leq MI = 0$ for some $n \in \mathbb{N}$. It follows by the given property of M that $AI^n = 0$. It will suffice therefore to show that AI^{k-1}/AI^k is finite for each $k \geq 1$ (where $I^0 = R$). Now AI^{k-1} is a finitely generated R-module because R, and hence A, is Noetherian; therefore AI^{k-1}/AI^k is a finitely generated R/I-module. As R/I is finite this now implies that AI^{k-1}/AI^k is finite. ■

Theorem 3.20 *Every finitely generated metabelian group is residually finite.*

Before proving this we make a useful observation. A group G is *monolithic if* G has a normal subgroup $M \neq 1$ such that *every non-identity normal subgroup* contains M, so M is the unique minimal normal subgroup (but the definition is stronger than that: it also requires that every normal subgroup $\neq 1$ does contain a minimal normal subgroup). In this case M is the *lith* of G.

Lemma 3.21 *If every monolithic quotient of a group G is finite then G is residually finite.*

Proof. Let $1 \neq a \in G$. The set

$$\mathcal{S} = \{K \lhd G \mid a \notin K\}$$

is non-empty since $a \neq 1$, and it is inductively ordered by inclusion, so by Zorn's Lemma it has a maximal member K. (If we are given that G satisfies max-n, this follows directly without ZL). The quotient G/K is monolithic with lith $K\left\langle a^G\right\rangle/K$, so G/K is finite. Thus G is residually finite. ■

Corollary 3.22 *Every finitely generated abelian group is residually finite.*

Proof. It's easy to see that a monolithic finitely generated abelian group is finite: Ex. sheet! ■

Proof. of Theorem *3.20* by the lemma, it will suffice to show that a monolithic finitely generated metabelian group G is finite.

If G is abelian this is easily proved by induction in the number of generators (Ex Sheet 3).

Suppose that G is not abelian, Let M be the lith of G, and set $A = G'$, $Q = G/A$, $R = \mathbb{Z}Q$. Then $A \neq 1$, so $A \geq M$. Since the R-submodules of A are precisely the normal subgroups of G contained in A, we are in the situation of Theorem 3.19. This now implies that A is finite.

Now by Lemma 3.15, G has a normal subgroup $N \geq A$ such that $\mathrm{C}_G(N) = \mathrm{Z}(N) := Z \geq N'$. Then $Z/(Z \cap A) \cong AZ/A$ is finitely generated, since G/A is a finitely generated abelian group. As A is finite it follows that Z is a finitely generated abelian group. If $m \in \mathbb{N}$ and $Z^m \neq 1$ then $Z^m \geq M$; but $\bigcap_{m\in\mathbb{N}} Z^m = 1$, so in fact $Z^m = 1$ for some m. It follows that $N^{m^2} = 1$. But N/A is a finitely generated abelian group as above, so N/A is finite, and so N is finite.

Therefore $G/\mathrm{C}_G(N) = G/Z$ is finite, and so finally G is finite. ■

An exercise on sheet 3 gives a 3-generator group G such that $G/\mathrm{Z}(G)$ is metabelian, but G is not residually finite. This shows that Theorem 3.20 is in one sense as good as it gets, if we are asking whether f.g. soluble groups are residually finite in more general. Next we'll consider a different kind of condition, which includes soluble groups of arbitrary derived length.

****

Polycyclic groups 1

Definition A group G is *polycyclic* if there is a finite series of subgroups

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G \tag{3}$$

such that G_i/G_{i-1} is cyclic for each i. Such a chain is called a *cyclic series*.

If $G_i = G_{i-1}\langle x_i\rangle$ for each i then $G = \langle x_1, \ldots, x_n\rangle$, so it is immediate that G in this case is generated by n elements.

Proposition 3.23 *The following are equivalent for a group G.*

(a) *G is soluble and every subgroup of G is finitely generated;*

(a*) *G is soluble and there exists $n \in \mathbb{N}$ such that every subgroup of G can be generated by n elements;*

(b) *G is soluble and satisfies* max*;*

(c) *G is polycyclic.*

Here *max* denotes the ascending chain condition for subgroups: *every strictly ascending chain of subgroups is finite.* The equivalence of (a) and (b) is a general feature of chain conditions (cf. *max-n* in an earlier section).

If G has a chain (3), $H \leq G$ and $N \lhd G$ then $(H \cap G_i)_{0 \leq i \leq n}$ and $(G_i N/N)_{0 \leq i \leq n}$ are chains in H and in G/N. Since

$$\frac{H \cap G_i}{H \cap G_{i-1}} \cong \frac{(H \cap G_i)G_{i-1}}{G_{i-1}} \leq \frac{G_i}{G_{i-1}} \tag{4}$$

and

$$\frac{(G_i N/N)}{(G_{i-1}N/N)} \cong \frac{G_i N}{G_{i-1}N} \cong \frac{G_i}{G_{i-1}(N \cap G_i)},$$

we see that both H and G/N are polycyclic: for subgroups and quotient groups of a cyclic group are cyclic.

In particular, H is can be generated by n elements; thus (c) implies (a*), which trivially implies (a). Conversely, given (a), we can refine the derived series of G to a series with cyclic factors. Say $D_i = \delta_i(G) = \langle y_{i1}, \ldots, y_{ik(i)} \rangle$; put $D_{ij} = D_{i+1} \langle y_{i1}, \ldots, y_{ik(i)} \rangle$; if $\delta_l(G) = 1$ then

$$\ldots D_{i+1} \lhd D_{i1} \lhd \ldots \lhd D_{ik(i)} = D_i \ldots \quad (l > i \geq 0)$$

is a series from 1 to G with each factor cyclic.

Corollary 3.24 *Every finitely generated nilpotent group is polycyclic.*

****

OMITTED

Polycyclic groups have many nice properties. These can usually be established by induction, using a measure of the 'size'. To define this we need

Lemma 3.25 *The number of factors G_i/G_{i-1} in (3) that are infinite depends only on G.*

This is immediate form the Jordan-Hölder Theorem, which says that two series like (3) have equivalent refinements (see 'Revision Notes'), and the fact that any series in an infinite cyclic group has exactly one infinite factor.

Definition Let G be a polycyclic group with a cyclic series (3). The number of infinite factors G_i/G_{i-1} is the *Hirsch length* $h(G)$ of G.

Lemma 3.26 *Let G be a group, $N \lhd G$ and $H \leq G$. Then G is polycyclic if and only if both N and G/N are polycyclic. In that case,*

(i) $h(G) = h(N) + h(G/N)$,

(ii) $h(H) \leq h(G)$ *and* $h(H) = h(G)$ *if and only if* $|G : H|$ *is finite.*

Proof. *(i)* Cyclic series in N and in G/N fit together to make a cyclic series in G; count infinite factors.

(ii) $h(H)$ is the number of infinite factors in the series $(H \cap G_i)$, which by (4) is no more than the number of infinite factors in the series (G_i). So $h(H) \leq h(G)$.

Suppose that $|G : H|$ is finite. Then H contains a normal subgroup N of finite index in G, and then

$$h(H) \geq h(N) = h(G) - h(G/N) = h(G),$$

so $h(H) = h(G)$.

Suppose conversely that $h(H) = h(G)$. Let $N \lhd G$. Then

$$\begin{aligned} h(N \cap H) + h(NH/N) &= h(N \cap H) + h(H/(N \cap H)) = h(H) \\ &= h(G) = h(N) + h(G/N). \end{aligned}$$

Since $h(N \cap H) \leq h(N)$ and $h(NH/N) \leq h(G/N)$ it follows that $h(N \cap H) = h(N)$ and that $h(NH/N) = h(G/N)$.

Now let's choose $N = G_{n-1}$ in (3), and suppose inductively that (ii) holds with N in place of G Then $h(N \cap H) = h(N)$ implies that $|N : N \cap H|$ is finite, and $h(NH/N) = h(G/N)$ implies that $|G : NH|$ is finite, as G/N is a cyclic group. Thus

$$|G : H| = |G : NH| \cdot |NH : H| = |G : NH| \cdot |N : N \cap H|$$

is finite. ■

****

Lemma 3.27 *If G is an infinite polycyclic group then G has an infinite free abelian normal subgroup.*

Proof. Let $D = \delta_m(G)$ be the last infinite term of the derived series of G (this exists because $\delta_0(G) = G$ is infinite and $\delta_l(G) = 1$ where l is the derived length of G). Then $D' = \delta_{m+1}(G)$ is finite. Put $C = \mathrm{C}_D(D')$. Then D/C is finite, and

$$[C', C] \leq [D', C] = 1,$$

so C is nilpotent of class at most 2. Let $Z = \mathrm{Z}(C)$. If Z is finite then C has finite exponent ('going-up' theorem for nilpotent groups), so D has finite exponent. As D/D' is a finitely generated abelian group this implies that D/D' is finite. But then D is finite, contradiction!

Therefore Z is infinite. Also Z is a finitely generated abelian group. Hence there exists $k \in \mathbb{N}$ such that Z^k is infinite and free abelian (for several different reasons: exercise!). Then $A := Z^k$ is the desired normal subgroup of G. ■

Theorem 3.28 *Every polycyclic group is residually finite.*

Proof. Let G be polycyclic and suppose that G is not residually finite. Then G has a normal subgroup N maximal subject to 'G/N is not residually finite'. Replacing G by G/N we may assume that every proper quotient group of G is residually finite.

Now G is infinite, so by the above lemma G has an infinite free abelian normal subgroup A. Then $1 \neq A^m \lhd G$ for each $m \in \mathbb{N}$, and so G/A^m is residually finite for each $m \in \mathbb{N}$. Thus the subgroups of finite index in G that contain A^m intersect in A^m. Hence the intersection of all the the subgroups of finite index in G is equal to $\bigcap_{m=1}^{\infty} A^m = 1$. So G is residuallty finite, contradicting the original assumption. ■

Remark: This argument shows more generally: If G has a family $\mathcal{X}$ of normal subgroups X such that G/X is residually finite, and $\bigcap \mathcal{X} = 1$, then G is residually finite. In fact for any property $\mathcal{P}$, 'residually residually $\mathcal{P}$' is the same as 'residually $\mathcal{P}$'; a group G is *residually* $\mathcal{P}$ if the normal subgroups X such that G/X has $\mathcal{P}$ intersect in $\{1\}$.

We will come back to polycyclic groups later in the next section.

4 Linear groups

A group is *linear* (of *degree* n) if it acts faithfully by linear transformations on a finite-dimensional (n-dimensional) vector space over a field, or if it is a group of linear transformations of such a vector space, or if it is a group of matrices over a field. These definitions are not identical, but they give the same groups up to isomorphism, and which meaning is intended is usually clear from the context (or doesn't matter).

k denotes a field and V a finite-dimensional vector space over k. Unless otherwise stated, $\dim_k(V) = n$.

Notation $\mathrm{GL}(V)$ is the group of all invertible linear transformations of V. Fixing a k-basis for V determines an isomorphism $\mathrm{GL}(V) \cong \mathrm{GL}_n(k)$, where $\mathrm{GL}_n(k)$, the *general linear* group, is the group of all invertible $n \times n$ matrices over k.

$\mathrm{SL}_n(k) = \{g \in \mathrm{GL}_n(k) \mid \det(g) = 1\}$ is the *special linear* group

$\mathrm{Tr}_n(k) = \{g \in \mathrm{GL}_n(k) \mid g_{ij} = 0 \ \ \forall i < j\}$ is the *lower-triangular* group

$\mathrm{U}_n(k) = \{g \in \mathrm{Tr}_n(k) \mid g_{ii} = 1 \ \ \forall i\}$ is the *lower unitriangular* group.

We take linear transformations to be acting on the *right*: given a basis $(e_1, \ldots, e_n)$ the matrix (g_{ij}) of $g \in \mathrm{GL}(V)$ is given by

$$e_i g = \sum_{j=1}^{n} g_{ij} e_j.$$

Until further notice, let $G \leq \mathrm{GL}(V)$. We consider $\mathrm{GL}(V)$ as contained in the k-algebra $\mathrm{End}(V)$ of all linear transformations of V, and sometimes identify $\mathrm{End}(V)$ with $\mathrm{M}_n(k)$, the algebra of all $n \times n$ matrices over k.

The subalgebra of $\mathrm{End}(V)$ generated by G will be denoted $k[G]$; this is just the linear span of G over k. There is an obvious ring epimorphism from the group algebra kG onto $k[G]$ (usually *not* an isomorphism, since the dimensions over k of these two algebras are respectively $|G|$ and n^2).

We will also *assume* until further notice that k is *algebraically closed*; since any field can be embedded in its algebraic closure, this is no great loss of generality. [WARNING: some of the results are *only valid under this hypothesis*, which I won't keep repeating. They remain valid in general if neither their hypothesis nor their conclusion is changed on embedding k into a larger field; this works e.g. for Lemma 4.9 but not for Proposition 4.3.]

V is a module for the group algebra kG in the obvious way. G is *irreducible* if V is simple as a kG-module, i.e. the only subspaces of V invariant under G are V and 0.

G is *completely reducible* if V is a direct sum of simple kG-modules.

It's often useful to break up a linear group into irreducible pieces, in the following way:

Proposition 4.1 *Let*

$$0 = V_0 < V_1 < \ldots < V_r = V \tag{5}$$

be a composition series for the kG-module V (i.e. each V_i/V_{i-1} is simple as a kG-module). Let $\pi_i : G \to \mathrm{GL}(V_i/V_{i-1})$ be the induced action of G on V_i/V_{i-1} for each i, and put $K = \bigcap_{i=1}^{n} \ker \pi_i$. Then each $\pi_i(G)$ is irreducible, G/K is isomorphic to a subgroup of $\pi_1(G) \times \cdots \times \pi_r(G) \leq \prod_{i=1}^{r} \mathrm{GL}_{n_i}(k)$, and $(K-1)^r = 0$.

This can be visualized if we pick a basis 'through the series (5)': let $(e_{11}, \ldots, e_{1n_1})$ be a basis for V_1, and having chosen a basis for V_{i-1} extend it to a basis for V_i by adding $(e_{i1}, \ldots, e_{in_i})$. W.r.t. this basis, each element of G takes the 'block-triangular' form

$$g = \begin{pmatrix} \pi_1(g) & 0 & \cdots & \cdots & \cdots & 0 \\ * & \ddots & 0 & & & \vdots \\ & * & \pi_i(g) & 0 & & \vdots \\ & & * & \ddots & 0 & \vdots \\ & & & * & \ddots & 0 \\ * & & & & * & \pi_r(g) \end{pmatrix}$$

where $\pi_i(g)$ denotes the matrix of g acting on V_i/V_{i-1} w.r.t. the basis $(e_{ij} + V_{i-1})$, and all entries above the diagonal are 0. Thus K consists of the 'block

lower unitriangular' matrices in G, and G/K is isomorphic to a group of block-diagonal matrices. Note that G/K is a completely reducible linear group: it acts faithfully on $V_1/V_0 \oplus \cdots \oplus V_r/V_{r-1}$, and each of these summands is simple as a module for $k(G/K)$.

If G is *completely reducible*, say $V = U_1 \oplus \cdots \oplus U_r$ where each U_i is a simple kG-submodule, we can *choose* $V_i = U_1 \oplus \cdots \oplus U_i$ and then G is represented by block-diagonal matrices.

Note: this proposition holds for *any* field k, not necessarily algebraically closed.

Lemma 4.2 *If G is abelian and irreducible then* $\dim_k(V) = 1$.

Proof. Let $0 \neq v \in V$. Then $V = vkG$ is isomorphic to kG/I where $I = \mathrm{ann}_{kG}(v)$. Since kG is commutative and kG/I has no proper right ideals, kG/I is a field. It is also an n-dimensional vector space over k; as k is algebraically closed this implies that $n = 1$. ■

Combined with the preceding Proposition this gives

Proposition 4.3 *If G is abelian then w.r.t. a suitable basis G is lower-triangular.*

An important feature of irreducible groups:

Proposition 4.4 *If G is irreducible then* $k[G] = \mathrm{End}(V)$. Equivalently*: G contains n^2 linearly independent matrices.*

Proof. OMITTED

****

Set $R = k[G] \subseteq E = \mathrm{End}(V) = \mathrm{M}_n(k)$, and identify k with $k\mathbf{1} \subseteq E$ where $\mathbf{1} = \mathbf{1}_n$ is the identity matrix. Let

$$S = \{y \in E \mid yr - ry \ \forall r \in R\}.$$

If $0 \neq y \in S$ then Vy is a non-zero R-submodule of V so $Vy = V$, and so y is invertible. Thus $k[y]$ is a subfield of E, hence a finite-dimensional extension field of k. As k is algebraically closed it follows that $k[y] = k$; thus $S = k\mathbf{1}$.

Suppose $\{w(1), \ldots, w(m)\}$ is a k-basis of R. Now a matrix $x = (x_{ij})$ belongs to S if and only if it satisfies the system of linear equations

$$\mathcal{S}: \quad \sum_l w(t)_{il} x_{lj} - \sum_l x_{il} w(t)_{lj} = 0 \quad (t = 1, \ldots, m)$$

in n^2 unkowns. Since $\dim_k(S) = 1$ it follows that $m \geq n^2 - 1$. If $m = n^2$ we are done.

Suppose $m = n^2 - 1$. Then $E = R \oplus wk$ for some w. Now

$$\frac{wR}{R \cap wR} \cong \frac{R + wR}{R} = \frac{E}{R} \cong k;$$

thus R has a 1-dimensional quotient module R/K where K is the annihilator in R of w modulo $R \cap wR$.

Claim: If $K < R$ is a right ideal of R then V is an epimorphic image of R/K.

Accepting the claim, it follows that $n = \dim_k(V) = 1$, and the result is clear.

Proof of claim: Let $0 \neq a \in V$ and put $I = \mathrm{ann}_R(a)$. Then $V = aR = \sum_{i=1}^{m} ag_i k$ for some $g_1, \ldots, g_m \in G$ (choose each $w(i) \in G$ w.l.o.g.). Put $I_j = g_1^{-1} I$ for each I. Then $R/I_j = R/\mathrm{ann}_R(ag_i) \cong V$ for each i, and

$$V \cdot (I_1 \cap \ldots \cap I_m) = 0,$$

so $I_1 \cap \ldots \cap I_m = 0$. Write $D_q = I_1 \cap \ldots \cap I_q$, and assume (after suitable relabelling) that $0 = D_r < D_{r-1} < \ldots < D_1 < D_0 = R$. For some $s \geq 1$ we have $D_s + K < R = D_{s-1} + K$. Then

$$0 \neq \frac{D_{s-1}}{D_s} = \frac{D_{s-1}}{D_{s-1} \cap I_s} \cong \frac{D_{s-1} + I_s}{I_s} \leq \frac{R}{I_s} \cong V$$

so $D_{s-1}/D_s \cong V$ since V is a simple module. On the other hand,

$$0 \neq \frac{R}{D_s + K} = \frac{D_{s-1} + K}{D_s + K} \cong \frac{D_{s-1}}{D_s + (D_{s-1} \cap K)},$$

a non-zero quotient of $D_{s-1}/D_s \cong V$, so it is isomorphic to V. Thus V is an epimorphic image of R/K. ■

****

Remarks. (1) The real import of the 'claim' is that all composition factors of R, as a module for itself, are isomorphic to V. This may be familiar from Representation Theory.

Corollary 4.5 *If G is irreducible then the only matrices commuting with all elements of G are the scalar matrices.*

Theorem 4.6 *Suppose that $G \leq \mathrm{GL}_n(k)$ is irreducible and that*

$$|\{\mathrm{tr}(g) \mid g \in G\}| = q < \infty.$$

Then $|G| \leq q^{n^2}$.

Proof. By the preceding theorem, G contains $m = n^2$ linearly independent matrices $w(1), \ldots, w(m)$. For $\underline{\mu} \in k^m$ let

$$G(\underline{\mu}) = \{g \in G \mid \mathrm{tr}(w(s)g) = \mu_s \ (s = 1, \ldots, m)\}.$$

Observe that $g = (g_{ij}) \in G(\underline{\mu})$ if and only if it satisfies the equations

$$\sum_{i=1}^{n} \sum_{l=1}^{n} w(s)_{il} g_{li} = \mu_s \quad (s = 1, \ldots, m).$$

This is a system of $m = n^2$ linearly independent equations, so it has at most one solution (g_{ij}). The result follows as there are just q^{n^2} possibilites for $\underline{\mu}$. ■

Corollary 4.7 *Suppose that $G \leq \mathrm{GL}_n(k)$ is completely reducible and that $g^e = 1\ \forall g \in G$. Then $|G| \leq e^{n^3}$.*

Proof. See Ex. sheet 3. ■

Proposition 4.8 ('Clifford's Theorem') *If G is irreducible and $N \lhd G$ then N is completely reducible.*

Proof. Let U be a non-zero kN-submodule of minimal dimension in the simple kG-module V. Then U is a simple kN-module, and so is Ug for each $g \in G$. Since $UkG = V$, we have $V = Ug_1 + \cdots + Ug_m$ for some $g_i \in G$.

Claim: if m is minimal then this sum is direct. For if $Ug_i \cap \sum_{j \neq i} Ug_j \neq 0$ then $Ug_i \leq \sum_{j \neq i} Ug_j$ since Ug_i is simple for kN, so Ug_i can be ommitted without changing the sum.

The result follows. ■

An element $g \in G$ is *unipotent* if $(g-1)^n = 0$ (where $n = \dim_k(V)$). The group G is *unipotent* if every element of G is unipotent. Thus K in Proposition 4.1 is a unipotent group.

Lemma 4.9 (i) *The following are equivalent, for an element $g \in G$:*

(a) *g is unipotent*

(b) *$(g-1)^m = 0$ for some $m \in \mathbb{N}$*

(c) *all eigenvalues of g are 1.*

(ii) *The group G is unipotent if and only if $(G-1)^n = 0$.*

Proof. (i) W.l.o.g. $G = \langle g \rangle$. Suppose (b) holds. Let v be an eigenvector with eigenvalue λ. Then $0 = v(g-1)^m = v(\lambda - 1)^m$ implies $\lambda = 1$, so (b) implies (c). Now suppose that (c) holds. Then the characteristic polynomial of g is $(t-1)^n$, and the Cayley-Hamilton Theorem implies that $(g-1)^n = 0$, so (c) implies (a).

(ii) 'If' is clear. Suppose that G is unipotent and irreducible. Then $\mathrm{tr}(g) = n$ for every $g \in G$, so $G = 1$ by Theorem 4.6. In the general case, we apply Proposition 4.1. Each of the images $\pi_i(G)$ is unipotent and irreducible, so $\pi_i(G) = 1$ for each i. It follows that $G = K$, whence the result. ■

Remark: this lemma, and the following theorem, do *not* require k to be algebraically closed. Although we used that assumption in the proof, neither hypothesis nor conclusion are affected if we enlarge the (arbitrary) field k to its algebraic closure.

This is a significant observation. Suppose $G \leq \mathrm{GL}_n(k)$ is unipotent, k being any field. If also G is *irreducible*, then claim (ii) implies that $G = 1$ (even though G might not a priori be irreducible as a linear group over the algebraic closure $\overline{k}$); for $V(G-1)$ is then a proper kG-submodule of V, so $V(G-1) = 0$. In general, it then follows by Proposition 4.1 that G is represented by unitriangular matrices over k, w.r.t. a suitable k-basis. In other words, for *any* field k,

- *every unipotent subgroup of $\mathrm{GL}_n(k)$ is conjugate to a unitriangular group.*

Theorem 4.10 *Let G be a unipotent subgroup of $\mathrm{GL}(V)$. Then*
(i) *G is nilpotent of class at most $n-1$;*
(ii) *if $\mathrm{char}(k) = 0$ then G is torsion-free;*
(iii) *if $\mathrm{char}(k) = p \neq 0$ then $g^{p^{n-1}} = 1$ for each $g \in G$.*

Proof. If $n = 1$ then $G = 1$. We suppose that $n \geq 2$ and argue by induction on n. We may as well assume that $G = \mathrm{U}_n(k)$. The result is easy to see 'by pictures'. There are two epimorphisms $\alpha,\ \beta : \mathrm{U}_n(k) \to \mathrm{U}_{n-1}(k)$, where

$$\alpha(g)_{ij} = g_{ij} \quad (1 \leq i, j \leq n-1),$$
$$\beta(g)_{ij} = g_{i-1,j-1} \quad (2 \leq i, j \leq n).$$

Clearly

$$\ker\alpha \cong \ker\beta \cong k_+^{n-1}$$

where k_+ denoted the additive group of k. Claims (ii) and (iii) now follow since $G/\ker\alpha \cong \mathrm{U}_{n-1}(k)$.

For claim (i), note that $g \in \ker\alpha \cap \ker\beta$ iff the only non-zero entry of $g - \mathbf{1}_n$ is g_{n1} in the bottom left-hand corner. It follows that $\ker\alpha \cap \ker\beta \leq \mathrm{Z}(G)$. Inductively we have $\gamma_{n-2}(G) \leq \ker\alpha \cap \ker\beta$, and so $\gamma_{n-1}(G) = 1$.

(All of this is a special case of 'stability group theory'). ■

Remark. This argument does not depend on the field k being algebraically closed; it show in general that a unipotent group G has a finite central series such that each factor is a subgroup of k_+.

Soluble linear groups

A linear group $G \leq \mathrm{GL}(V)$ is *triangularizable* if the kG-module V has a composition series with 1-dimensional factors (equivalently, a composition series of length n). Equivalently: G is represented by lower-triangular matrices w.r.t. some basis of V (or upper-triangular ones: this is equivalent: exercise!). Equivalently, if $G \leq \mathrm{GL}_n(k)$, G is triangularizable if there exists $\alpha \in \mathrm{GL}_n(k)$ such that $G^a \leq \mathrm{Tr}_n(k)$. (Recall: we are assuming that k is *algebraically closed*. For a general field k, one says that G is 'triangularizable' if it is so as a linear group over the algebraic closure $\overline{k}$ of k.)

If G is triangularizable then G' is unipotent, hence nilpotent. So G is soluble. We have seen already that the converse is true if G is *abelian.* In general, the converse is 'virtually' true – a group has a given property *virtually* if some normal subgroup of finite index has that property.

Theorem 4.11 (Lie-Kolchin-Mal'cev Theorem) *Let G be a soluble linear group of degree n. Then G has a triangularizable normal subgroup K of finite index at most $\mu(n)$, a number that depends only on n.*

Corollary 4.12 *Let G be a soluble linear group of degree n.*
(i) *G is virtually nilpotent-by-abelian;*
(ii) *the derived length of G is at most $\beta(n) := n + \log_2 \mu(n)$.*

Claim (ii) is *Zassenhaus's Theorem.*

Proof. of Theorem 4.11. If $n = 1$ we can take $\mu(n) = 1$. Let $n > 1$ and suppose inductively that $\mu(m)$ has been defined for all $m < n$.

We first consider some special cases.

Case 1: where

- every subgroup of index at most n in G is irreducible, and
- $G \leq \mathrm{SL}_n(k)$.

We will show that in this case, G is actually *finite*, with an explicit bound for its order.

By Lemma 3.15 G has a normal subgroup N such that

$$N' \leq \mathrm{Z}(N) = \mathrm{C}_G(N) := A.$$

By Clifford's Theorem both N and A are completely reducible. Let U be a simple kA-submodule of V; then $\dim_k U = 1$ by Lemma 4.2. Thus the action of A on U is given by

$$ua = \lambda(a)u$$

for $u \in U$ and $a \in A$, where $\lambda : A \to k^*$ is a homomorphism (a *character* of A). For each character χ of A let

$$W_\chi = \{v \in V \mid va = \chi(a)v \ \forall a \in A\};$$

thus $U \subseteq W_\lambda$.

If $g \in G$ and $v \in W_\chi$ then

$$(vg^{-1})a = v(a^g)g^{-1} = \chi(a^g)(vg^{-1}) \ \forall a \in A,$$

so $W_\chi g^{-1} \subseteq W_{\chi'}$ where $\chi'(a) = \chi(a^g)$; χ' is again a character of A, and the same calculation shows that $W_{\chi'}g \subseteq W_\chi$. Thus $W_\chi g^{-1} = W_{\chi'}$. So G permutes the submodules W_χ.

Since $UkG = V$ we have $V = Ug_1^{-1} \oplus \cdots \oplus Ug_n^{-1}$ for some $g_1, \ldots, g_n \in G$, where $g_1 = 1$ w.l.o.g.. Now suppose $0 \neq w \in W_\chi$. Then $w = \sum u_i g_i^{-1}$ for some $u_1, \ldots, u_n \in U$, where $u_j \neq 0$ for at least one j. Then for $a \in A$ we have

$$\sum \chi(a)u_i g_i^{-1} = \chi(a)w = wa = \sum \lambda(a^{g_i})u_i g_i^{-1},$$

and equating coefficients we deduce that $\chi(a) = \lambda(a^{g_j}) \ \forall a \in A$. Thus if $W_\chi \neq 0$ then $W_\chi = W_\lambda g_j^{-1}$, some $j \in \{1, \ldots, n\}$. Thus G permutes the subspaces $W_\lambda g_j^{-1}$. There are at most n of these, so the stabilizer H of W_λ has index at most n in G.

By hypothesis, H is irreducible. But $0 \neq U \subset W_\lambda \leq V$, and so $W_\lambda = V$. Thus A acts on V by scalar multiplication: $va = \lambda(a)v$. It follows that

$$1 = \det(a) = \lambda(a)^n$$

for all $a \in A$, whence $A^n = 1$, and in fact $|A| \leq n$ since k contains at most n nth roots of unity.

Since $A = \mathrm{Z}(N)$ and N is nilpotent of class ≤ 2 it follows that $N^{n^2} = 1$. Now Corollary 4.7 shows that $|N| \leq (n^2)^{n^3} = n^{2n^3}$. Finally, since G/A is isomorphic to a subgroup of $\mathrm{Aut}(N)$ it follows - very crudely - that

$$|G| \leq n(n^{2n^3})! := \psi(n).$$

Case 2:. Where every subgroup of index at most n in G is irreducible.

Put $Z = k^*\mathbf{1}_n$ and $G_2 = Z \cdot G$. If $g \in G$ and $\det g = \lambda$ then $\det(\lambda^{-1/n} g) = 1$, so $G_2 = Z \cdot G_1$ where $G_1 = G_2 \cap \mathrm{SL}_n(k)$. If $H \leq G_1$ and $|G_1 : H| \leq n$ then

$$|G : G \cap ZH| \leq |G_2 : ZH| = |ZG_1 : ZH| \leq |G_1 : H| \leq n,$$

so $G \cap ZH$ is irreducible, and so H is irreducible. It follows by Case 1 that $|G_1| \leq \psi(n)$. Thus $|G : G \cap Z| \leq |G_1| \leq \psi(n)$, and of course Z is triangularizable.

Case 3: Suppose that G has a reducible subgroup H of index at most n. Thus there is a kH-submodule U of V with $\dim_k(U) = a < n$ and $\dim_k(V/U) = n - a < n$. Let $\pi : H \to \mathrm{GL}(U)$ and $\rho : H \to \mathrm{GL}(V/U)$ be the corresponding representations. By inductive hypothesis, there exists triangularizable subgroups $H_1 \lhd \pi(H)$ and $H_2 \lhd \rho(H)$ with $|\pi(H) : H_1| \leq \mu(a)$ and $|\rho(H) : H_2| \leq \mu(n-a)$. Write $\theta = (\pi, \rho) : H \to \pi(H) \times \rho(H)$ and set $L = \theta^{-1}(H_1 \times H_2)$. Then L is a triangularizable normal subgroup of H, since composition series for kH_1 in U and for kH_2 in V/U fit together to give a composition series for kL in V.

Now $\theta(L) = (H_1 \times H_2) \cap \theta(H)$, so

$$\begin{aligned} |H : L| = |\theta(H) : \theta(L)| &\leq |\pi(H) \times \rho(H) : H_1 \times H_2| \\ &= |\pi(H) : H_1|\,|\rho(H) : H_2| \leq \mu(a)\mu(n-a). \end{aligned}$$

Hence $|G : L| \leq n\mu(a)\mu(n-a)$. Say $G = Hx_1 \cup \ldots \cup Hx_t$ (some $t \leq n$). Then $L \geq K := L^{x_1} \cap \ldots \cap L^{x_t}$ which is normal in G and satisfies

$$|G : K| \leq |G : L|^t \leq (n\mu(a)\mu(n-a))^n.$$

Conclusion: Putting together cases 2 and 3 we see that G has a triangularizable normal subgroup of index $\mu(n)$ if $\mu(n)$ is defined to be the supremum of the numbers

$$\psi(n),\ (n\mu(a)\mu(n-a))^n \quad (1 \leq a < n).$$

■

Linear groups over rings

Suppose that R is a subring of the field k. We denote by $\mathrm{GL}_n(R)$ the group of all invertible $n \times n$ matrices over R. This is exactly the stabilizer of $R^n \subseteq k^n$ within $\mathrm{GL}_n(k)$ (that is, the set of g such that $R^n g = R^n$.) A *linear group over* R is any group isomorphic to a subgroup of $\mathrm{GL}_n(R)$, for some n; equivalently, a group that acts faithfully by module automorphisms on some finitely generated free R-module.

Let I be an ideal of R. Then $\mathrm{GL}_n(R)$ fixes $I^{(n)}$ in R^n and has an induced action on the quotient $R^n/I^{(n)} \cong (R/I)^n$. (I write $I^{(n)}$ for $I \oplus \cdots \oplus I$ with n summands, to avoid confusion with the nth power of the ideal I.) So there is a homomorphism

$$\pi_I : \mathrm{GL}_n(R) \to \mathrm{Aut}_R((R/I)^n),$$

the group of R-module automorphisms of $(R/I)^n$. The kernel K_I of π_I consists of the matrices 'congruent to $\mathbf{1}_n$ modulo I', i.e.

$$K_I = \mathrm{GL}_n(R) \cap (\mathbf{1}_n + \mathrm{M}_n(I))$$

where $\mathrm{M}_n(I)$ denotes the set of $n \times n$ matrices with entries in I.

Lemma 4.13 *For each $s \geq 1$, there is an injective homomorphism*

$$\theta_s : K_{I^s}/K_{I^{s+1}} \to \mathrm{M}_n(I^s)/\mathrm{M}_n(I^{s+1}) \cong \mathrm{M}_n(I^s/I^{s+1})$$

(where the symbols on the right refer to additive groups of matrices).

Proof. Say $g = 1 + a,\ h = 1 + b \in K_{I^s}$. Then

$$\begin{aligned} gh &= 1 + a + b + ab \\ &\equiv 1 + a + b \mod I^{s+1} \end{aligned}$$

since $2s \geq s + 1$. Thus $g \longmapsto g - 1$ defines a homomorphism from K_{I^s} into the additive group $\mathrm{M}_n(I^s)$. If $h \in K_{I^{s+1}}$ then $gh \equiv 1 + a \mod I^{s+1}$, so this induces a homomorphism $\theta_s : K_{I^s}/K_{I^{s+1}} \to \mathrm{M}_n(I^s)/\mathrm{M}_n(I^{s+1})$. Clearly θ_s is injective since $(g-1) \in \mathrm{M}_n(I^{s+1})$ iff $g \in K_{I^{s+1}}$. ■

Theorem 4.14 *Suppose that R is Noetherian and that R/I is finite.*

(i) *The group $\mathrm{GL}_n(R)/K_{I^t}$ is finite for each $t \in \mathbb{N}$;*

(ii) *suppose further that $\bigcap_{t=1}^{\infty} I^t = 0$. Then $\mathrm{GL}_n(R)$ is residually finite;*

(ii) *suppose further that $pR \subseteq I$ where p is a prime number. Then K_I is residually a finite p-group.*

Proof. (i) Since R is Noetherian, each I^s is finitely generated as an ideal of R, so I^s/I^{s+1} is finitely generated as an R-module, and as it is annihilated by I it is a finitely generated R/I-module. Therefore I^s/I^{s+1} is finite. Now the preceding lemma implies that $K_{I^s}/K_{I^{s+1}}$ is finite if $s \geq 1$. Also $\mathrm{GL}_n(R)/K$ is isomorphic to a group of matrices over R/K, so $\mathrm{GL}_n(R)/K$ is finite. The claim follows.

(ii) The hypothesis implies that $\bigcap_{t=1}^{\infty} K_{I^t} = 1$, so this follows from (i).

(iii) Now for each s we have $pI^s \leq I^{s+1}$, and the lemma implies that $K_{I^s}/K_{I^{s+1}}$ has exponent dividing p, as well as being finite. It follows that K_I/K_{I^t} is a finite p-group for each $t \geq 1$. ■

Corollary 4.15 Let $G = \mathrm{GL}_n(\mathbb{Z})$.

(i) *G is residually finite;*

(ii) *For each prime p, G is virtually residually a finite p-group;*

(iii) *G is virtually torsion-free.*

Proof. (i) and (ii) follow from the theorem on taking $I = p\mathbb{Z}$. (iii) Let $p \neq q$ be primes. Then $H := K_{(p)} \cap K_{(q)}$ is residually finite-p and residually finite-q. Suppose $h \in H$ has finite order m. Then H has a normal subgroup H_1 such that $H_1 \cap \langle h \rangle = 1$ and H/H_1 is a p-group; then $m \mid p^e$ for some e. Similarly, $m \mid q^f$ for some f. It follows that $m = 1$, so $h = 1$. ■

The same result holds in greater generality; but this depends on some commutative algebra:

Theorem 4.16 *Let R be a finitely generated integral domain. Then R is Noetherian, and*

(i) *Every maximal ideal of R has finite index;*

(ii) *if I is a proper ideal of R then $\bigcap_{t=1}^{\infty} I^t = 0$;*

(iii) *the maximal ideals of R intersect in 0;*

(iv) *if $\mathrm{char}(R) = 0$ then for all but finitely many primes p there exist maximal ideals M with $\mathrm{char}(R/M) = p$.*

Proof. (Sketch) Hilbert's Basis Theorem shows that R is Noetherian. (i) Let $k = R/M$ be a field. The 'Weak Nullstellensatz' shows that k is a finite extension of its prime field F. If $F = \mathbb{Q}$ one could infer that $\mathbb{Q}$ is finitely generated as a $\mathbb{Z}$-algebra, which is false; therefore $F = \mathbb{F}_p$ for some prime p. (ii) Krull's Intersection Theorem. (iii) The 'Strong Nullstellensatz' says that R has the 'Jacobson property'.

(iv) For the main application in the following theorem, it's enough to show that at least *two* distinct primes occur as $\mathrm{char}(R/M)$; this follows immediately from (iii). For completeness we sketch the full proof: if $pR = R$ the p is a unit in R; a generalization of the Dirichet Units Theorem shows that the group R^* of units of R is finitely generated, while the 'fundamental theorem of arithmetic' says that the primes freely generate a free abelian group: it follows that an infinite set of primes can't be contained in the finitely generated group R^*. Thus almost all primes p satisfy $pR < R$, and then $pR \leq M < R$ for some maximal ideal M. ■

Theorem 4.17 *Let $G \leq \mathrm{GL}_n(k)$ be a finitely generated linear group. Then*

(i) *G is residually finite;*

(i)* *in fact, G is residually (finite and linear of degree n);*

(ii) *if $\mathrm{char}(k) = 0$ then G is virtually residually a finite p-group for all but finitely many primes p, and G is virtually torsion-free;*

(iii) *if $\mathrm{char}(k) = p \neq 0$ then G is virtually residually a finite p-group; G has a normal subgroup K of finite index such that every periodic subgroup of K is unipotent.*

Proof. Say $G = \langle g_1, \ldots, g_s \rangle$. Let R be the subring of k generated by all the entries of the matrices $g_1, g_1^{-1}, \ldots, g_s, g_s^{-1}$. Then $G \leq \mathrm{GL}_n(R)$. The residual properties now follow from the two preceding theorems. If K is residually a p-group then every element of finite order has order a power of p. In Case (iii) such elements are unipotent. In Case (ii), we argue as in the above corollary to show that G is virtually torsion-free.

For (i)*, note that if $1 \neq g \in G$ then $1 \not\equiv g \bmod I$ for some maximal ideal I of R so $g \notin \ker \pi_I$ where $\pi_I(G) \leq \mathrm{GL}_n(R/I)$, and R/I is a finite field. ■

Theorem 4.18 *Let G be a periodic linear group over a field k.*
(i) *If G is finitely generated then G is finite;*
(ii) *if $\mathrm{char}(k) = 0$ and G has finite exponent then G is finite.*

Proof. (i) If $\mathrm{char}(k) = 0$ this follows immediately from Theorem 4.17(ii).

Suppose that $\mathrm{char}(k) = p \neq 0$. By Theorem 4.17(ii), G has a unipotent normal subgroup K of finite index. Then K is finitely generated and nilpotent. Now K/K' is a finitely generated and periodic abelian group, so K/K' is finite. It follows that K is finite, by Corollary 3.11. Hence G is finite.

(ii) Now G has a unipotent normal subgroup K such that G/K is isomorphic to a completely reducible linear group (Proposition 4.1). But then K is torsion-free, so $K = 1$. Now Corollary 4.7 shows that $|G| = |G/K| \leq e^{n^3}$ if $G^e = 1$. ■

Remark. This does not depend on k being algebraically closed; we used that hypothesis in the proof of part (ii) [where?!], but neither the hypothesis nor the conclusion of the theorem are affected if we replace k by $\overline{k}$.

****

OMITTED

Induced representations

Lemma 4.19 *Suppose $H \leq G$ and $|G : H| = m < \infty$. If $H \leq \mathrm{GL}_n(R)$ then G is isomorphic to a subgroup of $\mathrm{GL}_{mn}(R)$.*

Proof. Let $\{1 = t_1, t_2, \ldots, t_m\}$ be a transversal to the right cosets of H in G, and let $V = R^n$ considered as an H-module. Now let $W = V_1 \oplus \cdots \oplus V_m \cong R^{mn}$ be the direct sum of m copies of the R-module V. We make G act on W by R-automorphisms as follows. First of all, $V_1 = V$ as RH-module. Next, for each i, t_i is an (R-module) isomorphism $V_1 \to V_i$. Thus we have $V_i = Vt_i$ for each i and

$$W = Vt_1 \oplus \cdots \oplus Vt_m.$$

Now for any $g \in G$, we have $t_i g = h(i,g)t_{j(i,g)}$ with $h(i,g) \in H$ and $j(i,g) \in \{1, \ldots, m\}$. Then we are forced to define the action of g on W by

$$vt_i \cdot g = vh(i,g)t_{j(i,g)} \quad (v \in V = V_1,\ 1 \leq i \leq m).$$

It's routine to verify that this gives a well-defined homomorphsim $\theta : G \to \mathrm{Aut}_R(W) \cong \mathrm{GL}_{mn}(R)$. Thus G permutes the summands $V_i = Vt_i$ ($i = 1, \ldots, m$). If $g\theta = 1_W$ then $Vt_1 = Vg = Vt_{j(1,g)}$ so $j(1,g) = 1$, whence $g = t_1 g = h(1,g)t_{j(1,g)} \in H$, and then $g = 1$ since H acts faithfully on $V = V_1$. Thus the action of G on W is faithful. ■

This shows that *every finite extension of an R-linear group is R-linear*. It is even easier to see that a *direct product* of finitely many R-linear groups is R-linear: If $H_i \leq \mathrm{Aut}_R(V_i)$, where $V = R^{n_i}$, then

$$H_1 \times \cdots \times H_m \leq \prod_1^m \mathrm{Aut}_R(V_i) \leq \mathrm{Aut}_R(V_1 \oplus \cdots \oplus V_m);$$

in matrix terms, $H_1 \times \cdots \times H_m$ is represented by block-diagonal matrices.

****

Polycyclic groups 2: Soluble $\mathbb{Z}$-linear groups

Now we specialize further to $R = \mathbb{Z}$.

Theorem 4.20 *Let $G \leq \mathrm{GL}_n(\mathbb{Z})$. If G is abelian then G is finitely generated.*

This depends on a non-trivial theorem of algebraic number theory:

Theorem 4.21 'Dirichlet Units Theorem' *Let R be the ring of integers of an algebraic number field. Then the group of units R^* of R is finitely generated.*

(This is actually the easier part of the 'Units Theorem'; the full result also specifies the torsion-free rank (i.e. Hirsch length) of R^*. We don't need this here.)

Proof. of Theorem 4.20. Let $V = \mathbb{Q}^n$ considered as a $\mathbb{Q}G$-module. We argue by induction on n, and consider two cases.

Case 1. Where V is not simple as a $\mathbb{Q}G$-module. Say $0 < U < V$ where U is $\mathbb{Q}G$-submodule of V. Write $L = \mathbb{Z}^n$. Then $L \cap U$ spans U and $(L+U)/U$ spans V/U, so $L \cap U \cong \mathbb{Z}^m$ and $(L+U)/U \cong \mathbb{Z}^{n-m}$ where $0 < m = \dim_{\mathbb{Q}}(U) < n$.

Thus $G/\mathrm{C}_G(L \cap U)$ is isomorphic to a subgroup of $\mathrm{GL}_m(\mathbb{Z})$ and $G/\mathrm{C}_G((L+U)/U)$ is isomorphic to a subgroup of $\mathrm{GL}_{n-m}(\mathbb{Z})$. Applying the inductive hypothesis we may suppose that both $G/\mathrm{C}_G(L \cap U)$ and $G/\mathrm{C}_G((L+U)/U)$ are finitely generated.

Now consider $C = \mathrm{C}_G(L \cap U) \cap \mathrm{C}_G((L+U)/U)$. Since $(L+U)/U \cong L/(L \cap U)$ as G-modules, 'stability group' theory (Ex sheet) shows that C is isomorphic to a subgroup of $(L \cap U)^{n-m} \cong \mathbb{Z}^{m(n-m)}$. So C is finitely generated. Also G/C is isomorphic to a subgroup of $G/\mathrm{C}_G(L \cap U) \times G/\mathrm{C}_G((L+U)/U)$, so G/C is finitely generated. Hence G is finitely generated.

Case 2. Where V is simple as a $\mathbb{Q}G$-module. Let $0 \neq u \in V$. Then

$$V = u\mathbb{Q}G \cong \mathbb{Q}G/I$$

where $I = \mathrm{ann}_{\mathbb{Q}G}(u)$ is an ideal of $\mathbb{Q}G$. Since V is a simple $\mathbb{Q}G$-module, I is a maximal ideal of $\mathbb{Q}G$ and so $\mathbb{Q}G/I := F$ is a field. Also $\dim_{\mathbb{Q}}(F) = \dim_{\mathbb{Q}}(V) = n$, so F is a finite extension of $\mathbb{Q}$, that is, an algebraic number field.

Write $\widetilde{g} = g + I$ for the image in F of $g \in G$. Then $g \longmapsto \widetilde{g}$ is a homomorphism, and it is injective since

$$\widetilde{g} = 1 \Longleftrightarrow g - 1 \in I \Longleftrightarrow u(g-1) = 0 \Longleftrightarrow V(g-1) = 0 \Longleftrightarrow g = 1.$$

Let $g \in G$. The characteristic polynomial χ_g of g is monic and has coefficients in $\mathbb{Z}$, and the Cayley-Hamilton Theorem says that $\chi_g(g) = 0$. Then $\chi_g(\widetilde{g}) = 0$, so $\widetilde{g}$ is an algebraic integer. Since $g^{-1} \in G$ we also find that $\widetilde{g}^{-1}$ is an algebraic integer. Thus $\widetilde{g} \in R^*$ where R is the ring of integers of F.

Thus $\widetilde{G} \leq R^*$. Now R^* is finitely generated by the Units Theorem, hence so is its subgroup $\widetilde{G}$, hence so is G since $G \cong \widetilde{G}$. ■

Lemma 4.22 *Let A be a finitely generated abelian group. Then $\mathrm{Aut}(A)$ is linear over $\mathbb{Z}$.*

Proof. Note first (a) every finite group is linear over $\mathbb{Z}$: for $\mathrm{GL}_n(\mathbb{Z})$ contains a copy of the symmetric group $Sym(n)$ consiting of the permutation matrices (which act by permuting the elements of the standard basis of $\mathbb{Z}^n$).

(b) a direct product of two linear groups (over a given ring) is linear: represent (g, h) by the block-diagonal matrix $\begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}$.

Now the torsion subgroup T of A is finite. For some $m \in \mathbb{N}$ we have $A^m \cap T = 1$ (why?). Let $\Gamma = \mathrm{Aut}(A)$. Then Γ acts on A/T and on A/A^m, and the natural homomorphism

$$\Gamma \to \mathrm{Aut}(A/T) \times \mathrm{Aut}(A/A^m)$$

is injective since

$$[a, \gamma] \in T \ \& \ [a, \gamma] \in A^m \quad \Longrightarrow [a, \gamma] = 1.$$

Now $A/T \cong \mathbb{Z}^n$ for some n, so Δ is linear over $\mathbb{Z}$, and $\mathrm{Aut}(A/A^m)$ is finite. it follows by (a) and (b) above that Γ is linear over $\mathbb{Z}$. ■

Theorem 4.23 *Let G be a soluble group. If every abelian subgroup of G is finitely generated then G is polycyclic.*

Proof. Induction on the derived length l of G. If $l \leq 1$ then G is abelian and there is nothing to prove. Suppose that $l > 1$, and put $A = \delta_{l-1}(G)$. It will suffice to show that every abelian subgroup of G/A is finitely generated: if this is the case, then by inductive hypothesis G/A will be polycyclic, and the result will follow since A is abelian and (therefore also) finitely generated.

So let B/A be an abelian subgroup of G/A, and put $C = \mathrm{C}_B(A)$. Then B/C is isomorphic to a subgroup of $\mathrm{Aut}(A)$, so B/C is linear over $\mathbb{Z}$. Also $B' \leq A \leq C$, so B/C is finitely generated, by Theorem 4.20.

Note now that C is nilpotent since $B' \leq A \leq \mathrm{Z}(C)$. Let $D \geq A$ be a maximal abelian normal subgroup of C. Then $D = \mathrm{C}_C(D)$ and is D is finitely generated; thus C/D is isomorphic to a subgroup of $\mathrm{Aut}(D)$, and so C/D is linear over $\mathbb{Z}$. Also C/D is abelian since $A \leq D \leq C \leq B$; it follows as above that C/D is

finitely generated. Putting all together we deduce that B is finitely generated as required. ■

Remarks. (i) The converse of this theorem was included in Proposition 3.23.

(ii) In fact it's enough to assume that every 2-*step subnormal* abelian subgroup is finitely generated: exercise! (A is 2-*step subnormal* in G if $A \lhd K \lhd G$ for some K.)

Now combining this with Theorem 4.20 we get the generalization:

Theorem 4.24 *Every soluble linear group over $\mathbb{Z}$ is polycyclic.*

It is also true, conversely, that *every polycyclic group is linear over* $\mathbb{Z}$ (theorem of L. Auslander). Thus we have a beautiful characterization of this class of groups. For the proof, see Chapter 5 of my book 'Polycyclic groups'. If we assume it, then the next result is immediate from Corollary 4.12. But we can prove it directly (actually the logic goes the other way: Theorem 4.25 is required as the first step in proving Auslander's theorem):

Theorem 4.25 *Every polycyclic group is virtually nilpotent-by-abelian.*

Proof. Let G be polycyclic and suppose that G is not virtually nilpotent-by-abelian. Let N be maximal among the normal subgroups of G such that G/N is not virtually nilpotent-by-abelian. To get a contradiction, we may now replace G by G/N and so assume: every proper quotient group of G is virtually nilpotent-by-abelian. Now G is infinite (as it is not virtually trivial), so G has an an infinite free abelian normal subgroup A. Say $A \cong \mathbb{Z}^d$. The conjugation action of G on A gives a homomorphism $\theta : G \to \mathrm{GL}_d(\mathbb{Z}) \cong \mathrm{Aut}(A)$.

By Theorem 4.11, $\theta(G)$ has a normal subgroup K of finite index such that K is triangularizable over $\mathbb{C}$. Then K' is unipotent, so $(K'-1)^d = 0$. It follows that $B := \mathrm{C}_A(K') > 0$.

Now (reverting to multiplicative notation) $1 \neq B \lhd G$, so G/B is virtually nilpotent-by-abelian. Thus G/B has a normal subgroup G_1/B of finite index such that $\gamma_n(G_1') \leq B$ for some n. Put $H = G_1 \cap \theta^{-1}(K)$. Then $H \lhd G$, $|G:H| \leq |G:G_1|\,|\theta(G):K| < \infty$, and $\gamma_{n+1}(H') \leq [\gamma_n(G_1'), H'] \leq [B, K'] = 1$. So G is virtually nilpotent-by-abelian, the required contradiction. ■

Remark: a direct, but slightly longer, version of the same argument goes like this: G has a finite series of normal subgroups $1 = G_0 \leq G_1 < \ldots < G_m \leq G$ such that G/G_m is finite and $G_i/G_{i-1} = A_i \cong \mathbb{Z}^{d_i}$ for each i. The conjugation action of G on these factors gives homomorphisms $\theta_i : G \to \mathrm{GL}_{d_i}(\mathbb{Z}) \cong \mathrm{Aut}(A_i)$, and Theorem 4.11 provides a normal subgroup H of finite index in G such that $\theta_i(H')$ is unipotent for each i. Then

$$A_i \left(\theta_i(H') - 1\right)^{d_i} = 0$$

for each i. This now implies that $[[\ldots[G_i, H'], \ldots,]H'] \leq G_{i-1}$ for each i, and hence that $\gamma_n((H \cap G_m)') = 1$ where $n = d_1 + \cdots + d_m$.