Group Theory

§0. Intro & Notation.

$H \leq G$ subgroup

$H < G$ proper subgroup

$H \trianglelefteq G$ normal subgroup.

Def H is subnormal in G if $\exists$ chain $H = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = G$.
The least such n is called the defect of H.

If $\alpha : G \to H$ is a group homomorphism, write g^α for the image of g under α. (the hom. law is then $(g_1 g_2)^\alpha = g_1^\alpha g_2^\alpha$).

Def the center of G is $Z(G) := \{ g \in G : gx = xg \ \forall x \in G \}$.
(it is an abelian normal subgroup of G).

$\mathrm{Aut}(G) :=$ group of all automorphisms of G.

$\mathrm{Inn}(G) :=$ group of all inner automorphisms of G (i.e $\{ g^\tau : x \mapsto x^g = g^{-1}xg \ , g \in G \}$)
$(\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G))$

The outer automorphism group is $\mathrm{Out}(G) = \mathrm{Aut}(G) / \mathrm{Inn}(G)$.

Obs: there is an exact sequence

$$\begin{tikzcd}
1 \arrow[r] & Z(G) \arrow[r] & G \arrow[r, "\tau"] \arrow[dr] & \mathrm{Aut}(G) \arrow[r] & \mathrm{Out}(G) \arrow[r] & 1 \\
 & & & \mathrm{Inn}(G) \arrow[u] & &
\end{tikzcd}$$

Def. (semidirect product): Let $N \triangleleft G$, $H \leq G$, $H \cap N = \{1\}$, $H \cdot N = G$.
We say that G is the semidirect product of H and N.

Properties:

i) $x \in G \Rightarrow x = hn$ for unique $h \in H$, $n \in N$.

ii) Let $h \in H$, define $h^\alpha : N \to N$ by $n \mapsto h^{-1} n h = n^h$ $(\alpha : H \to \mathrm{Aut}(N))$.

iii) If we are given groups H, N and an hom. $\alpha : H \to \mathrm{Aut}(N)$, we can define the external semidirect product, $H \ltimes_\alpha N$.

Def: (of ext. semi-dir. prod): $G = H \ltimes_{\alpha} N$ is a group with underlying set $H \times N$, with group operation $(h_1, n_1)(h_2, n_2) = (h_1 h_2, n_1^{h_2^{\alpha}} n_2)$

(motivation: in the internal, $(h_1, n_1)(h_2, n_2) = h_1 h_2 h_2^{-1} n_1 h_2 n_2 = (h_1 h_2) \cdot (n_1^{h_2} n_2)$)

$(1_H, 1_N)$ the identity, and need to check associativity.

$(hn)^{-1} = n^{-1} h^{-1} = h^{-1} h n^{-1} h^{-1} = h^{-1} (n^{-1})^{h^{-1}}$ (internal).

In the external, $(h,n)^{-1} = \left(h^{-1}, (n^{-1})^{(h^{-1})^{\alpha}}\right)$.

Rk: if $\alpha : H \to \operatorname{Aut} N$ is trivial ($h^{\alpha} = 1_{\operatorname{Aut}(N)}\ \forall h$) then $G \overset{\text{as groups!}}{\cong} H \times N$.

Now we identify $G = H \ltimes_{\alpha} N$ as an internal semidirect product.

Let $\tilde{H} := \{(h, 1_N) : h \in H\} \leq G$ $(\tilde{H} \cong H)$ and

$\tilde{N} := \{(1_H, n) : n \in N\} \trianglelefteq G$ $(\tilde{N} \cong N)$.

Note $\tilde{H} \cap \tilde{N} = 1$, $G = \tilde{H}\tilde{N}$ (check everything works).

Example: Let $N = \langle a \rangle \times \langle b \rangle$, $(a^2 = b^2 = 1)$

$H = \langle h \rangle$.

$\alpha : H \to \operatorname{Aut}(N)$ by $h^{\alpha} : \begin{cases} a \mapsto b \\ b \mapsto ab \end{cases}$

Can check that $G = H \ltimes N \cong A_4$

- Wreath product:

Let H, K be any two groups.

Def: (The standard wreath product) of H and K is $W := H \overset{\text{order matters!}}{\operatorname{wr}} K$.

First, define $B := \{$ restricted functions $f : K \to H \}$ (i.e. $f(k) = 1_H$ for all but finite $k \in K$).

$(fg)(k) := f(k) \overset{\text{multiplication!}}{\cdot} g(k)$

Write $f \in B$ as $(f_k)_{k \in K}$ (as it were a sequence, $f_k = f(k)$).

Let then, for $k \in K$, $h \in H$, define $f_{k,h} \in B$ by:

$f_{k,h}(k) = h$ and $f_{k,h}(k') = 1_H$ for $k' \neq k$ (support of f of only k).

Let $H_k := \{f_{k,h} : h \in H\} \leq B$.

We can see $H_k \simeq H$ by $f_{k,h} \mapsto h$, and $B = \mathrm{Dr}_{k \in K} H_k$

(D_r is the restricted direct product, or direct sum $\oplus$).

Define $\alpha : K \to \mathrm{Aut}(B)$ by k^α s.t. $(f^{k^\alpha})_{k_1} = f_{k_1 k^{-1}}$ $(k \in K)$

Check that $k^\alpha \in \mathrm{Aut}(B)$, and that α is an homomorphism.

(In fact, k^α permutes the H_{k_1}'s by right multiplication on K.

Let $k', k_1 \in K$ and let $f \in H_k$ s.t.

$$(f^{k'^\alpha})_{k_1} = f_{k_1(k')^{-1}} = 1 \text{ iff } k_1(k')^{-1} \neq k$$

(i.e. $k_1 \neq kk'$.) Thus, $f^{(k')^\alpha} \in H_{kk'}$, and $H_k^{(k')^\alpha} = H_{kk'}$.

For simplicity, write $f^{k'}$ for $f^{(k')^\alpha}$.

The wreath product is $W := K \underset{\alpha}{\times} B$.

(if K and H are finite, $|W| = |B||K| = |H|^{|K|} \cdot |K|$.

Exercise: identify $\mathbb{Z}_2$ wr $\mathbb{Z}_2$.

Theorem: Suppose $H \neq 1$ and K infinite. Then $Z(H \text{ wr } K) = 1$.

Pf $W = H \text{ wr } K$. Then $W = KB$, $B \trianglelefteq W$ and $K \cap B = 1$.

Let $z \in Z(W)$, and write $z = kf$ $(k \in K, f \in B)$. Then

$H_{1_K} = H_{1_K}^z = (H_{1_K}^k)^f = H_k^f = H_k$ since $H_k \trianglelefteq B$. Thus $k = 1_K$ and $z = f \in B$.

Now, let $k_1 \in K$. Then $f^{k_1} = f$, so $f_{xk_1^{-1}} = f_x$ $\forall k_1 \in K$.

Thus f is constant on K, so ($f = 1$ a.e) $f(x) = 1_H$ $\forall x \in K$, and $f = 1_W$ //

Application:

Def A (possibly infinite) group G is a p-group (p prime) if each element of G has order a power of p.

(for G finite, this is equivalent to saying that $|G| = p^{\alpha}$ for some α, by Lagrange + Cauchy).

Recall: for G finite p-group of order > 1, $|Z(G)| > 1$. This is false for infinite p-groups!

Theorem: There is an infinite (solvable) p-group G with $Z(G) = 1$.

Pf Choose H cyclic of order p, and let K be an infinite elementary abelian p-group (a direct sum of $\mathbb{Z}/p\mathbb{Z}$'s). Let $G = H \text{ wr } K$. Then $Z(G) = 1$ by previous theorem.

Also, B is a p-group, and so is $G/B \simeq KB/B \simeq K$.

(a power of p puts you in B, another power kills you). (in fact, p^2 is enough)

It is solvable because B is abelian and G/B is also abelian. //

- Composition series, Jordan-Hölder thm, simple groups.

Def. A series in a group G is a chain of subgroups:

$$\mathcal{S} : 1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

The G_i are the terms of the series, and G_{i+1}/G_i are called the factors. The length of $\mathcal{S}$ is the number of nontrivial factors.

(also called normal or subnormal series. It can be generalized to admit an ∞-length series).

If $\mathcal{S}, \mathcal{Z}$ are two series in G and if each term of $\mathcal{S}$ is a term of $\mathcal{Z}$, we say that $\mathcal{Z}$ is a refinement of $\mathcal{S}$.

Def a composition series in G is $\mathcal{S}$ such that it as no proper refinements.

Finite groups have composition series, always.

Lemma: Let $\mathcal{S}$ be a series in G. Then $\mathcal{S}$ is a composition series iff each non-trivial factor is a simple group.

Schreier's refinement theorem: Any two series in G have isomorphic refinements (two series are isomorphic if there is a bijection between their sets of factors such that corresponding groups are isomorphic).

Proof: use Zassenhauss's lemma.

Jordan-Hölder Theorem: Any two composition series in a group G are isomorphic

Def: The composition factors of a group G (with a composition series) are the factors of a composition series (unique up to permutation and isomorphism).

Rk: S_3 and $\mathbb{Z}/6\mathbb{Z}$ have the same composition factors.

Def: (acc): a group G satisfies the ascending chain ~~condition~~ for subnormal groups if there is no infinite ascending chain.
(i.e. $\nexists$ $H_1 < H_2 < \cdots$ where each H_i is a subnormal subgroup of G.
(dcc): the same but with descending chains.

Examples:

i) Any finite group satisfies both acc and dcc.
ii) $\mathbb{Z}$ satisfies acc but not dcc.
iii) Simple groups satisfy dcc and acc.
iv) Let G be the mult. group of all complex $2^{th}, 4^{th}, 8^{th} \ldots$ roots of unity. If $H < G$, then H is finite. Thus G satisfies dcc, but not acc.

Theorem: A group G has a composition series iff it satisfies both acc and dcc for $\underbrace{\text{subnormal}}_{(sbl)}$ subgroups.

Pf/ ⇒) Assume G has a comp. series of length ℓ.

Suppose $\exists$ a chain of subnormal sgps with length $\ell+1$.

$$H_1 < H_2 < \cdots < H_{\ell+1} \quad \text{(each } H_i \text{ subnormal in } G)$$

Note that H_i sbl $G \Rightarrow H_i$ sbl H_{i+1} (intersect with H_{i+1}!).

So we can refine the chain to a series of length $\geq \ell+1$.

By the refinement theorem, this series and the comp. series have isomorphic refinements, so ⇒⇐!! Hence G satisfies acc & dcc.

⇐) Assume G satisfies acc & dcc.

Consider the set of proper normal subgroups of G. This has a maximal element (otherwise $\exists$ infinite a.c. of normal subgroups!).

Pick H_1 maximal. So G/H_1 is simple.

Repeat the argument for H_1 (if it is trivial, we are done).

This procedure leads to a descending chain

$$G = H_0 \supsetneq H_2 \supsetneq H_3 \supsetneq \cdots \cdots \quad \text{with } H_i/H_{i+1} \text{ sbl. By dcc, it terminates} //$$

Hölder program

To classify all finite groups we need to:

(i) Find all simple groups.

(ii) Solve the extension problem:

Let N, Q be finite groups Q simple.

Describe all extensions of N by Q: $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$

Some simple groups

i) The abelian simple groups are just the groups of prime order.

ii) The alternating groups, $n \geq 5$ are simple.

iii) Infinite simple groups:

Lemma: Let $\{G_\lambda : \lambda \in \Lambda\}$ be a chain of simple subgroups of G.

Then $\bigcup_{\lambda\in\Lambda} G_\lambda$ is simple.

Pf/ Put $\mathcal{U} := \bigcup_{\lambda\in\Lambda} G_\lambda$, $1 \neq N \lhd \mathcal{U}$. want to show $N = \mathcal{U}$.

Let $x \in N$, $x \neq 1$. So $x \in G_{\lambda_0}$ for some $\lambda_0 \in \Lambda$.

So $x \in G_\lambda \ \forall G_\lambda \geq G_{\lambda_0}$

Then $1 \neq x \in N \cap G_\lambda \lhd G_\lambda \overset{G_\lambda \text{ simple}}{\Rightarrow} N \cap G_\lambda = G_\lambda \Rightarrow G_\lambda \subseteq N$ for all $G_\lambda \geq G_{\lambda_0}$

So $N = \mathcal{U}$.

//

Application:

Define $\mathfrak{S} = \mathrm{Sym}\{1, 2, 3, \dots\}$.

Regard A_n as a subgroup of $\mathfrak{S}$ (fixing all $m > n$).

We get $A_5 \lneq A_6 \lneq \cdots \lneq A_n \lneq A_{n+1} \leq \cdots$

Put $\mathcal{U} = \bigcup_{n\geq 5} A_n$, then $\mathcal{U}$ is simple and infinite. (called the infinite Alternating Gp)

//

iv) Projective groups:

Recall: Let F be a field, then $GL_n(F)$ is the general linear group of deg n over F. (nonsingular $n \times n$ matrices over F).

The map $\overset{\in GL_n(F)}{A} \mapsto \det A$ is a gp homomorphism $\overset{\det AB = \det A . \det B}{}$ (surjective to $F^* = F \setminus \{0\}$).

The kernel is $SL_n(F) = \{A \in GL_n(F) : \det A = 1_F\}$.

is called the Special Linear Group. $(SL_n(F) \lhd GL_n(F))$.

Exercise: $Z(SL_n(F))$ is the group of scalar matrices $\{c \cdot 1\!\!1_n ,\ c \in F^*,\ c^n = 1\}$.

Define $PSL_n(F) := SL_n(F) / Z(SL_n(F))$

It is called the Projective Special Linear group. (connection with projective geom.)

Theorem: the group $PSL_n(F)$ is simple if $n > 2$, and if $n = 2$, $|F| > 3$.

Pf (only for $n=2$, $|F| > 3$)

The key is:

Lemma: Let $N \triangleleft SL_n(F)$. If N contains a transvection (a matrix $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$, $c \neq 0$), then $N = SL_n(F)$.

Pf It is enough to show that N contains all transvections $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

If it does,
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -x & 1 \end{pmatrix} \in N$$

$\Rightarrow$ N contains all transvections.

But using elementary matrix operations can reduce any (2×2) matrix to its normal form, which is a product of transvections ($\Rightarrow \in N$)

Let $0 \neq x \in F$. Then N contains
$$\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix}$$

So if $0 \neq x, y \in F$, N contains
$$\begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & ay^2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a(x^2 - y^2) \\ 0 & 1 \end{pmatrix}$$

If $\mathrm{char}(F) \neq 2$, take $b \in F$. $b = \left(\frac{b+1}{2}\right)^2 - \left(\frac{b-1}{2}\right)^2 = x^2 - y^2 \Rightarrow$ ✓.

If $\mathrm{char}(F) = 2$, then $F = F^2 \Rightarrow$ ax^2 is a general element in $F \Rightarrow$ ✓.

(if F is not perfect last line is not true but we can still solve it).

//

(cont proof):

To prove the theorem, now it is enough to show that, if $N \trianglelefteq SL_2(F)$ and $N \not\leq Z SL_2(F)$, then $N = SL_2(F)$.

Let N be such a normal subgroup. ← can assume N contains no transvection. Take $A \in N$, $A \notin Z(SL_2(F))$ (i.e. A is not a scalar matrix).

The Rat. Canonical Form of A is either $\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$ $(a \neq a^{-1})$ or $\begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}$ (because $\det A = 1$).

As A is similar to its RCF, can assume A is one of the two matrices.

Case $A = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$: put $B := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(F)$.

Then N contains $A^{-1} \cdot (B^{-1} A B) = \begin{pmatrix} 1 & 1-a^2 \\ 0 & 1 \end{pmatrix}$ is a transvection $\Rightarrow$!!

so need $1 - a^2 = 0$, $a^2 = 1$ so $A = \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in Z(SL_2(F))$.

Case $A = \begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}$: let $x \in F$, put $B := \begin{pmatrix} 1 & -x^2 \\ 0 & 1 \end{pmatrix}$.

Then N contains $A(B^{-1} A^{-1} B) = \begin{pmatrix} 1 & -x^2 \\ -x^2 & 1+x^4 \end{pmatrix}$ $(*)$

Hence N contains

$$\begin{pmatrix} x^{-1} & x^{-1} \\ 0 & x \end{pmatrix}^{-1} \begin{pmatrix} 1 & -x^2 \\ -x^2 & 1+x^4 \end{pmatrix} \begin{pmatrix} x^{-1} & x^{-1} \\ 0 & x \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2+x^4 \end{pmatrix} \quad (\forall x \in F).$$

So N contains, $\forall x, y \in F$,

$$\begin{pmatrix} 0 & 1 \\ -1 & 2+x^4 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 2+y^4 \end{pmatrix} = \begin{pmatrix} 1 & x^4 - y^4 \\ 0 & 1 \end{pmatrix}$$

As N contains no transvection, $x^4 - y^4 = 0 \ \forall x, y \in F \overset{y=1}{\Rightarrow} x^4 = 1 \ \forall x \in F$

$\Rightarrow |F| = 5$ (otherwise, it is a contradiction)

Take $x = 1$ in $(*)$. Get $X := \begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix} \in N$. Let $Y := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

So N contains $\left(Y(X^{-1} Y^{-1}) X\right) = \begin{bmatrix} 1 & -2 \\ -2 & 0 \end{bmatrix}$ (since $F = \mathbb{F}_5$). Conjugate by $\begin{pmatrix} 2 & -1 \\ -2 & -1 \end{pmatrix}$ to get $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in N$

Now $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \Rightarrow$!!

//

Example: Let F be a finite field of order q. We write $GL_n(q)$ instead of $GL_n(F)$ and so on.

$$\# GL_n(q) = (q^n-1)\cdot(q^n-q)(q^n-q^2)\cdots\cdots(q^n-q^{n-1})$$

Because
$$1 \to SL_n(q) \to GL_n(q) \xrightarrow{\alpha} \overbrace{GF(q)^*}^{\#=q-1} \to 1$$

$(\alpha: A \mapsto \det A)$ so $\# SL_n(q) = \dfrac{\# GL_n(q)}{(q-1)}$

$Z(SL_n(q))$ = set of scalar matrices.

$$\begin{pmatrix} c & & 0 \\ & \ddots & \\ 0 & & c \end{pmatrix} \qquad \det(\ ) = c^n = 1.$$

So $\# Z(SL_n(q)) = \gcd\{q-1, n\}$. (using that $GF(q)^*$ is cyclic of order $q-1$)

Hence $\# PSL_n(q) = \dfrac{\# SL_n(q)}{\gcd\{q-1,n\}}$.

For $n=2$:

- if q is even, $\# PSL_2(q) = (q-1)q\cdot(q+1)$.
- if q is odd, $\# PSL_2(q) = \dfrac{(q-1)q(q+1)}{2}$.

Can check that $PSL_2(2) \cong S_3$, $PSL_2(3) \cong A_4$.

$\# PSL_2(4) = 60$ and is A_5

$\# PSL_2(5) = 60$ and is A_5

$\# PSL_2(7) = 168$. new! ← gp. of projectivities of the proj. plane with 7 points.

$\# PSL_2(8) = 504$. new!

$\# PSL_2(9) = 360 = \dfrac{6!}{2}$ ← it is A_6

Called "coincidence"

∘ Classification of finite simple groups.

The finite simple groups are:

- groups of prime order.
- alternating groups A_n.
- projective groups
- symplectic groups
- orthogonal groups
- unitary groups

& 26 sporadic groups.

§2. Solvable and Nilpotent groups.

Def A group G is *solvable* (or soluble) if it has a series with abelian factors ($1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ with G_{i+1}/G_i abelian).

The length of a shortest such series is called the *derived length*.

(gp of derived length $\leqslant 1$ are the abelian groups).

The groups of derived length $\leqslant 2$ are called *metabelian*.

Def A group G is *nilpotent* if it has a *normal* series

($1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ and $G_i \triangleleft G \ \forall i$)

Such that $G_{i+1}/G_i \leqslant Z(G/G_i)$

Such a series is called a *central series*.

The length of a shortest central series is called the *nilpotence class* of G.

Note that abelian $\Rightarrow$ nilpotent $\Rightarrow$ solvable.

Also:

1) D_8 = Dihedral (8) (of order 8) is nilpotent with class 2 ($\Rightarrow$ not abelian).

2) S_3 is solvable, but not nilpotent because $Z(S_3) = 1$.

Examples of finite nilpotent groups and solvable groups.

<u>Theorem</u>: Let p, q, r be primes.

i) if $|G| = p^m$, then G is nilpotent. If $m > 0$, then the nilpotence class of G is $\leq m-1$.

ii) if $|G| = p^m q$, $p^2 q^2$ or pqr, then G is solvable.

Pf (i) $|G| = p^m$, $m > 0$ (for $m = 0$, trivial).

Construct the <u>upper central series</u> in G:

Let $G_0 = 1$, put $G_1 = Z(G)$. Then G_1 is not trivial (from the class equation)

If $G_1 \neq G$, define $G_2/G_1 = Z(G/G_1)$. Get $G_2 > G_1 > G_0 = 1$

Eventually - since G is finite, will find some $G_n = G$.

For the nilpotence class, need the following lemma:

<u>Lemma</u>: if $H/Z(H)$ is cyclic, then H is abelian.

Suppose $G_{m-1} \neq G$. Then $1 < G_1 < \dots < G_{m-1} < G_m$, and $|G_{m-1}| \geq p^{m-1}$

Since $|G| = p^m$, $|G_{m-1}| = p^{m-1}$. Now $Z(G/G_{m-2}) = \frac{G_{m-1}}{G_{m-2}}$, and

So $\frac{(G/G_{m-2})}{Z(G/G_{m-2})} = \frac{G/G_{m-2}}{G/G_{m-1}} \cong G/G_{m-1}$ cyclic $\Rightarrow$ by lemma, G/G_{m-2} is abelian.

But then $G/G_{m-2} = Z(G/G_{m-2}) = \frac{G_{m-1}}{G_{m-2}} \Rightarrow G = G_{m-1} \Rightarrow !!$ //

<u>Corollary</u> (to (i)): if $H < G$, then $H < N_G(H)$. (if $|G| = p^m$).

Pf Use the series $1 = G_0 \leq G_1 \leq \dots \leq G_{m-1} = G$. Since $H \neq G$, there is a least i s.t $G_i \not\leq H$. Then $G_{i-1} \leq H$.

Note that $H \triangleleft HG_i$ (because $G_i/G_{i-1} = Z(G/G_{i-1}) \Rightarrow H/G_{i-1} \triangleleft HG_i/G_{i-1}$).

But at the same time, $G_i \not\leq H$. So $H < N_G(H)$. //

(continues proof of theorem).

(ii) Will do the case $|G| = p^m \cdot q$.

It's enough to show that each composition factor of G has prime order. Each such factor has order $| p^m q$. We can assume the that G is simple.

Let P be a Sylow p-subgroup of G $(|P| = p^m)$.

By Sylow's th., if n_p is the number of Sylow p-subgroups, $n_p \equiv 1 \bmod p$, and also $n_p \mid |G:P| = q$.

$n_p \neq 1$ because G is simple, and so $n_p = q$

Choose P_1, P_2, two different Sylow p-sgp s.t. $|P_1 \cap P_2|$ is maximal.

Write $I := P_1 \cap P_2$.

<u>Case</u> $I = 1$: Then every pair of Sylow p-sgps intersect at 1. To count the number of p-elements (elts of order power of p), is $(p^m - \underset{\overset{\uparrow}{id}}{1})q + \overset{id}{1}$ $= p^m q - q + 1$. This leaves $p^m q - (p^m q - q + 1) = q - 1$ elts of order power of q $\Rightarrow$ only one Sylow q-sbgp $\Rightarrow \trianglelefteq G \Rightarrow !!$.

<u>Case</u> $I \neq 1$.

Let $N_i := N_{P_i}(I)$, $i = 1, 2$. Note $I \neq P_1$, $I \neq P_2$ because otherwise would have $P_i \subseteq P_j \Rightarrow P_i = P_j \Rightarrow !!$.

Hence $I < N_1$, $I < N_2$ (by $\overset{\text{previous}}{}$ corollary).

Put $J := \langle N_1, N_2 \rangle \leqslant G$. Then $I \triangleleft J$

Suppose that J is a p-group. Then J is contained in some Sylow p-sbgp. P_3.

Then $P_1 \cap P_3 \geqslant P_1 \cap J \geqslant P_1 \cap P_2 = I$. If $P_1 \cap P_3 = I$, then leads a contradiction, and otherwise I is not maximal. So J is <u>not</u> a p-group.

$\uparrow$ Note that $P_1 \cap P_3 \geqslant P_1 \cap J \geqslant P_1 \cap N_1 = N_1$ $\Rightarrow N_1 \leqslant I \Rightarrow N_1 = I \Rightarrow !!$

$\downarrow$

(cont pf)

Then $|J| \mid p^m q \Rightarrow q \mid |J|$.

Let Q be a Sylow q-sgp of J. $|Q| = q$.

Next, $|QP_1| = \frac{|Q||P_1|}{|Q \cap P_1| = 1} = p^m q = |G| \Rightarrow G = QP_1$

This means, if we write $I^G = \langle I^g : g \in G \rangle$ (normal closure)

then $1 \neq I^G$, also $I^G \trianglelefteq G$. And $G = QP_1$. As $I \trianglelefteq \overset{\text{as}}{J}$, $(Q \subseteq J)$

then $I^{QP_1} = I^{P_1} \leq P_1 < G \Rightarrow I^G$ is proper normal $\Rightarrow$!! //

Exercise: prove the other cases.

Comments:

1) Every group of order $p^m q^n$ is solvable. (Burnside).

2) Groups of order $p^2 q r$ needn't be solvable. (e.g. A_5).

Examples (from ring theory).

Let R be a ring with identity, and let S be a subring which is nilpotent (as ring) (i.e $S^n = 0$, $n > 0$, where S^n = additive sgp generated by all $s_1 \cdot s_2 \cdots s_n$, $s_i \in S$)

↑ in fact, a subring.

Define $\mathcal{U} := \{ 1 + s, s \in S \} \subseteq R$.

Claim: $\mathcal{U}$ is a group wrt ring multiplication.

$(1+s_1)(1+s_2) = 1 + (s_1 + s_2 + s_1 s_2) \in \mathcal{U}$.

$(1+s)^{-1} = 1 - s + s^2 - s^3 + \cdots + (-1)^{n-1} s^{n-1}$ (because $S^n = 0$) //

Claim: $\mathcal{U}$ is nilpotent (group). (of class $n-1$).

Define $\mathcal{U}_r := \{ 1 + s, s \in S^r \}$ (S^r: sgp generated by $s_1 \cdots s_r$, $s_i \in S$).

(check $\mathcal{U}_r \leq \mathcal{U}$, and $\mathcal{U}_n = 1$, and $1 = \mathcal{U}_n \leq \mathcal{U}_{n-1} \leq \cdots \leq \mathcal{U}_2 \leq \mathcal{U}_1 = \mathcal{U}$)

Let $x \in S^r$, $y \in S^s$. We will show that $[1+x, 1+y] \in \mathcal{U}_{r+s}$

↓

(continues with example).

Compute $[1+x,1+y] = (1+x)^{-1}(1+y)^{-1}(1+x)(1+y) = ((1+y)(1+x))^{-1}(1+x)(1+y)$

Put $a := x+y+xy$; $b := x+y+yx$.

Then $(1+x)(1+y) = 1+a$, $(1+y)(1+x) = 1+b$.

So $[1+x,1+y] = (1+b)^{-1}(1+a) = (1-b+b^2-b^3+\cdots+(-1)^{n-1}b^n)(1+a)$

Rewrite this as $[1+x,1+y] = 1+(1-b+b^2\cdots+(-1)^{n-2}b^{n-2})(a-b)+(-1)^{n-1}b^{n-1}a$

Notice that $b^{n-1}a \in S^n$ $(a,b \in S)$. So $b^{n-1}a = 0$.

Also, $a-b = xy-yx \in S^{r+s}$. So $[1+x,1+y] \in U_{r+s}$.

In particular, letting $s=1$, $1+y$ is a general element of U, and

$$\underbrace{[1+x,1+y] \in U_{r+1}}_{\Downarrow\ U_{r+1} \trianglelefteq G\ \forall r} . \text{ So } U_r/U_{r+1} \leq Z(G/U_{r+1})$$

So the series $1 = U_n \leq U_{n+1} \leq \cdots \leq U_1 = U$ is a central series of G, of length $\leq n-1$.

So G is a nilpotent group of class $\leq n-1$.

Application: rings of matrices.

Let R be any ring with identity (not necessarily commutative).

Let $S := M_n(R)$, ring of all $n\times n$ matrices over R, and let N be the subring of S consisting of all upper zero triangular matrices.

$$\begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$$ (zeros on and below the diagonal).

(note the change in notation used (N is the previous S), S is the previous R, ...)

Note that $N^n = 0$ (N^i consists of matrices with $i-1$ superdiagonals $=0$).

In this case, $\mathcal{U}$ is the group of upper unitriangular $n\times n$ matrices over R.

$$\begin{pmatrix} 1 & * & * \\ & \ddots & * \\ 0 & & 1 \end{pmatrix}.$$ We write $\mathcal{U}$ as $\mathcal{U}_n(R)$.

<u>Fact</u>: $\mathcal{U}_n(R)$ is nilpotent of class $= n-1$ ($\leq$ by previous, but easy to see $=$).

Write $T_n(R) =$ group of $n\times n$ invertible triangular $n\times n$ matrices over R.

(i.e. $\begin{pmatrix} \text{unit} & & * & * \\ & \text{unit} & & * \\ & & \text{unit} & * \\ 0 & & & \ddots \\ & & & & \text{unit} \end{pmatrix}$)

~~Note that there is a homomorphism $\theta : T_n(R) \longrightarrow \mathrm{Units}(R)$~~

~~$A \longmapsto \det(A)$~~

~~with $\operatorname{Ker} \theta =$~~

There is a surjective gp homomorphism $\theta : T_n(R) \twoheadrightarrow \underbrace{\mathrm{Units}(R) \times \cdots \times \mathrm{Units}(R)}^{(n)}$

$$\begin{pmatrix} u_1 & * & * \\ & \ddots & * \\ 0 & & u_n \end{pmatrix} = A \longmapsto (u_1, \ldots, u_n)$$

And $\operatorname{Ker} \theta = \mathcal{U}_n(R)$.

So $T_n(R) \big/ \mathcal{U}_n(R) \cong (\mathrm{Units}(R))^n \leftarrow$ an <u>abelian</u> gp if R is commutative.

So ~~that~~ $T_n(R)$ is a soluble group, for any R commutative with 1.

<u>Example</u>:

(i) Let $R = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, for p a prime.

Then $\#\mathcal{U}_n(p) := \#\mathcal{U}_n(\mathbb{F}_p) = p^{\binom{n}{2}}$,

$\#T_n(p) = p^{\binom{n}{2}} \cdot (p-1)^n$.

(ii) Let $R = \mathbb{Z}$. Get $\mathcal{U}_n(\mathbb{Z})$, $T_n(\mathbb{Z})$ are infinite.

$\mathcal{U}_n(\mathbb{Z})$ is a torsion-free nilpotent group (no nontrivial elements of finite order).

(For it note that $\mathcal{U}_i/\mathcal{U}_{i+1} \cong \underbrace{\mathbb{Z}^+ \oplus \cdots \oplus \mathbb{Z}^+}_{n-i}$: f-gen torsion free.)

Note that $T_n(\mathbb{Z})/U_n(\mathbb{Z}) \simeq \mathrm{Unit}(\mathbb{Z}) \times \overset{n}{\cdots} \times \mathrm{Unit}(\mathbb{Z}) \simeq (\pm 1)^n \simeq (\mathbb{Z}/2\mathbb{Z})^n \in$ finite!

So $|T_n(\mathbb{Z})/U_n(\mathbb{Z})| = 2^n$.

Commutator Calculus

Let $x_1, x_2, \ldots$ elements of a group G.

Def The commutator of x_1, x_2 is $[x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2$.

More generally, one can define a supercommutator of weight $n (\geq 1)$ by:

$[x_1] := x_1$

$[x_1, x_2, \ldots, x_{n+1}] := [[x_1, \ldots, x_n], x_{n+1}]$ (called right-normed commutator)

Basic identities:

Let $x, y, z \in G$.

(i) $[x,y]^{-1} = [y,x]$

(ii) $[xy, z] = [x,z]^y [y,z]$ $\qquad (a^x = x^{-1} a x)$

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

(iii) $[x, y^{-1}] = \left([x,y]^{(y^{-1})}\right)^{-1}$.

(iv) $[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$ (Hall-Witt identity).

Pf (i) - (iii) exercise.

(iv) Put $u := x z x^{-1} y x$

$v := y x y^{-1} z y$

$w := z y z^{-1} x z$

Then $u^{-1} v = x^{-1} y^{-1} x z^{-1} x^{-1} y x y^{-1} z y = y^{-1} (\underbrace{y x^{-1} y^{-1} x}_{[x,y^{-1}]^{-1}} \underbrace{z^{-1}}_{z^{-1}} \underbrace{x^{-1} y x y^{-1}}_{[x,y^{-1}]} \underbrace{z}_{z}) y = [x, y^{-1}, z]^y$

So we want to prove that $(u^{-1}v).(v^{-1}w)(w^{-1}.u) = 1$ which is obvious.

//

- Commutators of Subgroups

Let $X_1, X_2, \ldots$ be nonempty subsets of a group G. Define

Df The commutator subgroup of weight n, $[X_1, \ldots, X_n]$ is,

$[X_1] := \langle X_1 \rangle$

$[X_1, X_2] := \langle [x_1, x_2] \mid x_1 \in X_1,\ x_2 \in X_2 \rangle$

And $[X_1, \ldots, X_{n+1}] := \Big[[X_1, \ldots, X_n], X_{n+1}\Big]$.

The derived chain

Example: define $[G,G] =: G'$, the derived subgroup of G.

Df The derived chain of subgroups of G is $G^{(i)}$, $i=0,1,\ldots$ by:

$G^{(0)} = G$, $G^{(i+1)} := \left(G^{(i)}\right)'$

Then $G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots$

Note that $G^{(i)} \lhd G$.

Lemma: Let $H, K \leqslant G$, with $K \lhd G$ and H characteristic in K (i.e. $H = H^{\alpha}$ $\forall \alpha \in \mathrm{Aut}(K)$). Then $H \lhd G$.

(characteristic is a stronger form of normality, which is transitive).

Pf Let $g \in G$. Then $K = K^{g}$, so g induces an automorphism in K (by conjugation).

So $H^{g} = H \Rightarrow H \lhd G$. //

Now, if $K \lhd G$, then $K' \lhd G$, because K' is characteristic in K, since $K' = \langle [x,y] \mid x, y \in K \rangle$, and $[x,y]^{\alpha} = [x^{\alpha}, y^{\alpha}] \in K'$.

Proposition: Let G be a soluble group (finite or infinite), with a series

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G, \text{ with } G_{i+1}/G_i \text{ abelian.}$$

Then $G^{(i)} \leq G_{n-i}$ $(0 \leq i \leq n)$.

(So for a soluble group, $G^{(n)} = 1$).

Corollary: The derived length of G equals the length of the derived series.

Corollary: A soluble group has a normal series with abelian factors.

Pf (of proposition): induction on i. ($i=0$ ok).

Assume that $G^{(i)} \leq G_{n-i}$.

since G_{n-i}/G_{n-i-1} is abelian

$$G^{(i+1)} \left(= [G^{(i)}, G^{(i)}]\right) = (G^{(i)})' \leq (G_{n-i})' \leq G_{n-i-1}$$

- The upper and lower central chains

Let G be a group.

Define the lower central chain:

$$\gamma_1(G) = G; \quad \gamma_{i+1}(G) := [\gamma_i(G), G]$$

So $G = \gamma_1(G) \geq \underset{\substack{\shortparallel \\ G'}}{\gamma_2(G)} \geq \cdots$

Define the upper central chain:

$$Z_0(G) = 1; \quad Z_{i+1}(G)/Z_i(G) = Z\left(G/Z_i(G)\right).$$

So $1 = Z_0(G) \leq \underbrace{Z_1(G)}_{\substack{\shortparallel \\ Z(G)}} \leq \cdots$

Note: $\gamma_i(G) \trianglelefteq G$ and $Z_i(G) \trianglelefteq G$.

Proposition: Let G be a nilpotent group (a group with a central series)

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G \qquad \left(\text{so that } G_i \trianglelefteq G, \text{ and } G_{i+1}/G_i \leq Z(G/G_i)\right)$$

Then:

(i) $\gamma_i(G) \leq G_{n-i+1} \quad 1 \leq i \leq n+1$

(Hence $\gamma_{n+1}(G) = 1$).

(ii) $G_i \leq Z_i(G) \quad 0 \leq i \leq n$

(Hence $Z_n(G) = G$)

Pf/ Prove (i), and (ii) is done similarly:

Induction on i (clear if $i=1$).

If $\gamma_i(G) \leq G_{n-i+1}$

Then $\gamma_{i+1}(G) = [\gamma_i(G), G] \leq [G_{n-i+1}, G] \underset{\substack{\uparrow \\ \text{because } G_{n-i+1}/G_{n-i} \subseteq Z(G/G_{n-i})}}{\leq} G_{n-i}$

Corollary: The nilpotence class of G equals:

1) The length of the upper central series.
2) The length of the lower central series.

Exercise: The Dihedral group $\mathrm{Dih}(2^r)$ (of order 2^r) is nilpotent. Find its nilpotence class.

Rk: every finite p-group is nilpotent (because the upper central series will reach G), as $G \neq 1 \Rightarrow Z(G) \neq 1$.

Proposition:

Let G be any group, ~~H~~ $X, Y \overset{\swarrow \text{subsets}}{\subseteq} G$; $H, K, L \leq G$.

(i) $[X,K]^K = [X,K]$ $\qquad \left(X^Y = \langle x^y \mid x \in X, y \in Y \rangle \right)$.

So if X is a subgroup, $[H,K] \trianglelefteq \langle H, K \rangle$.

(ii) If $K = \langle Y \rangle$, then $[H,K] = [H,Y]^K$

(iii) (Three subgroup lemma). If any two of $[H,K,L]$, $[K,L,M]$, $[L,H,K]$ are contained in some $N \trianglelefteq G$, then so is the third.

Pf

(i) Let $x \in X$, $k_1, k_2 \in K$.

$$[x, k_1 k_2] = [x, k_2][x, k_1]^{k_2} \Rightarrow [x, k_1]^{k_2} = [x, k_2]^{-1}[x, k_1 k_2] \in [X, K] \checkmark$$

(ii) Let $h \in H$, $k \in K$. Can write k in terms of Y, as $k = y_1^{\varepsilon_1} y_2^{\varepsilon_2} \dots y_r^{\varepsilon_r}$ $(y_i \in Y, \varepsilon_i = \pm 1)$

Show that $[h,k] \in [H,Y]^K$ by induction on r

$\underline{r=1}$: $[h, y_1] \in [H,Y]^K$.

$$[h, y_1^{-1}] = \left([h, y_1]^{-1}\right)^{y_1^{-1}} \in [H,Y]^K.$$

$\underline{r > 1}$

$$[h,k] = [h, (y_1^{\varepsilon_1} \dots y_{r-1}^{\varepsilon_{r-1}}) y_r^{\varepsilon_r}] = \overbrace{[h, y_r^{\varepsilon_r}]}^{r=1} \overbrace{[h, y_1^{\varepsilon_1} \dots y_{r-1}^{\varepsilon_{r-1}}]}^{\text{induction step}}{}^{y_r^{\varepsilon_r}} \in [H,Y]^K.$$

(iii) $[H,K,L] = \underbrace{[[H,K],L]}_{\shortparallel}$ and $[H,K] = \langle [h, \overset{\swarrow \text{can put either } k \text{ or } k^{-1}}{k^{-1}}] , h \in H, k \in K \rangle$.

By (ii), $\overset{[L,[H,K]]}{[H,K,L]}$ is generated by conjugates of $[[h,k^{-1}],l]$

The same is true for the other ~~two~~ commutators.

$[K,L,H]$ by conjugates of $[k, l^{-1}, h]$

By the Hall-Witt identity,

$[h, k^{-1}, l]^k [k, l^{-1}, h]^l [l, h^{-1}, k]^h = 1$, so $[h, k^{-1}, l]$ is a product of conjugates of $[k, l^{-1}, h]$, $[l, h^{-1}, k]$.

Now suppose $[K,L,H]$ and $[L,H,K] \leq N \trianglelefteq G$.

So $[h,k^{-1},l] \in N$ $\forall\, h\in H, k\in K, l\in L$.

So all conjugates are in N also. As $[H,K,L]$ is generated by conjugates of these, ✓. //

<u>Corollary</u>: If two of $[H,K,L]$, $[K,L,H]$, $[L,H,K]$ is trivial $(=\{1\})$, then the third is also. (take $N=1$).

<u>Corollary</u>: If $H,K,L \trianglelefteq G$, then $[H,K,L] \leq [K,L,H][L,H,K]$ (take $N:=[K,L,H][L,H,K]$)

- <u>Properties of upper and lower central chains</u>

<u>Theorem</u> Let G be any group.

(i) $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$.

(ii) $\gamma_i(\gamma_j(G)) \leq \gamma_{ij}(G)$.

(iii) $[\gamma_i(G), Z_j(G)] \leq Z_{j-i}(G)$ $(j\geq i)$

(iv) $G^{(i)} \leq \gamma_{2^i}(G)$

Pf (i) Use induction on j:

if $j=1$, $[\gamma_i(G), G] = \gamma_{i+1}(G)$ by definition.

If true for j, $[\gamma_i(G), \gamma_j(G)] \leq [\gamma_{i+j}(G)]$

$$[\gamma_i(G), \gamma_{j+1}(G)] = [\gamma_i(G), [\gamma_j(G), G]] = [[\gamma_j(G),G], \gamma_i(G)]$$

Apply the 3 sgp lemma as in 2nd corollary.

So $[[\gamma_i(G);G], \gamma_i(G)] \leq [G, \gamma_i(G), \gamma_j(G)][\gamma_i(G), \gamma_j(G), G] =$

$\overset{\text{induction}}{\leq} [\gamma_{i+1}(G), \gamma_j(G)] \cdot [\gamma_{i+j}(G), G] \overset{\text{induction}}{\leq} \gamma_{i+1+j}(G) \cdot \gamma_{i+j+1}(G) = \gamma_{i+j+1}(G)$ //

(cont pf)

(ii) & (iii) as exercise.

(iv) want $G^{(i)} \leq \gamma_{2^i}(G)$. Note that it is true for $i=0$. Induction.

$$G^{(i+1)} = \left(G^{(i)}\right)' = \gamma_2\left(G^{(i)}\right) \leq \gamma_2\left(\gamma_{2^i}(G)\right) \overset{\text{by (ii)}}{\leq} \gamma_{2^{i+1}}(G).$$

//

Corollary: Let G be a nilpotent gp of class $c \geq 1$.

Then the derived length of G is $\leq \lceil \log_2 c \rceil + 1$

Pf/ By hypothesis, $\gamma_{c+1} = 1$.

Let i be least s.t. $2^i \geq c+1$. Then $G^{(i)} \leq \gamma_{2^i}(G) \leq \gamma_{c+1}(G) = 1$

(so $i = \lceil \log_2 c \rceil + 1$).

//

Example: Let R be a commutative ring with identity, $T_n(R)$ the triangular matrices.

We saw that $T_n(R)$ is solvable, and that $U_n(R) \trianglelefteq T_n(R)$ and $U_n(R)$ nilpotent, and $T_n(R)/U_n(R)$ is abelian

We saw that $U_n(R)$ has nilpotence class $\leq n-1$ $(n \geq 2)$

$\Rightarrow U_n(R)$ has derived length $\leq \lceil \log_2(n-1) \rceil + 1$ $(n \geq 2)$

So the derived length of $T_n(R)$ will be $\leq \lceil \log_2(n-1) \rceil + 2$.

§3. Nilpotent Groups.

Let G be any group. Form the lower central series $G_i := \gamma_i(G)$.

$G = G_1 \geq G_2 \geq \cdots\cdots$, $G_i \trianglelefteq G$

Put $F_i := G_i / G_{i+1}$, the ith factor.

$F_1 = G_1/G_2 = G/[G,G] = G/G'$, the abelianization of G.

Question: is there a relation between F_1 and the subsequent factors?

Theorem: There is a surjective homomorphism from $F_i \underset{(\mathbb{Z})}{\otimes} \overset{F_1}{\overset{\shortparallel}{G_{ab}}} \twoheadrightarrow F_{i+1}$,

via the map $(aG_{i+1}) \otimes (gG') \longmapsto [a,g]\,G_{i+2}$

Pf/ The map $(aG_{i+1}, gG') \longmapsto [a,g]G_{i+2}$ is well defined:

Because of the commutator identities ($[ab,c]$ and $[a,bc]$).

$[G_{i+1}, G] = G_{i+2}$.

$[G_i, G'] = [\gamma_i(G), \gamma_2(G)] \leq \gamma_{i+2}(G)$.

Show it is balanced (middle-linear) i.e.: $[ab,x]\,G_{i+2} = ([a,x]G_{i+2})([b,x]G_{i+2})$

$[a,xy]\,G_{i+2} = ([a,x]G_{i+2})([a,y]G_{i+2})$

$[ab,x] = [a,x]^b[b,x] = [a,x]\underbrace{[a,x,b]}_{\substack{\uparrow \\ [G_i, G, G_i] \leq G_{i+1+i} \subseteq G_{i+2}\ \checkmark}}[b,x]$

(the other done similarly).

By the univ. mapping property, we have an homomorphism.

It is surjective because $[a,x]G_{i+2}$ generate $G_{i+1}/G_{i+2} = F_{i+1}$. //

Corollary (1) $G_i/_{G_{i+1}}$ is a homomorphic image of $G_{ab} \otimes \underset{i}{\cdots} \otimes G_{ab}$ (by induction on i).

Corollary (2) Let $\mathbb{P}$ be a property of groups which is inherited ~~by~~ under:

→ tensor products (of abelian groups)

→ homomorphic images (i.e. quotients)

→ extensions ($N \trianglelefteq G$ and N and $G/_N$ have $\mathbb{P}$, then G has $\mathbb{P}$).

Let G be a nilpotent group such that G_{ab} has $\mathbb{P}$. Then G has $\mathbb{P}$.

Pf/ By corollary (1), each $G_i/_{G_{i+1}}$ has property $\mathbb{P}$.

If G has nilpotent class c, then $G_{c+1} = 1$.

$$1 = G_{c+1} \trianglelefteq G_c \trianglelefteq \cdots \trianglelefteq G_1 = G$$

hence (by inheritence ~~[illegible]~~ by extensions) G has $\mathbb{P}$. //

Examples:

1. $\mathbb{P}$: "being finite": A nilpotent group G is finite iff G_{ab} is finite.
2. $\mathbb{P}$: "being finitely generated": A nilpotent group G is fg iff G_{ab} is f.g.

- Elements of finite order in nilpotent groups.

Recall: in an abelian group, the set of elements of finite order is a subgroup.

Not true in general groups (not even for soluble, as $Dih(\infty)$ is!).

Example: The infinite ~~[illegible]~~ dihedral group ($Dih(\infty)$): $\langle x\rangle \ltimes \langle a\rangle$

where a has infinite order, $|x| = 2$ and $a^x = a^{-1}$.

Note $(xa)^2 = xaxa = x^2(x^{-1}ax)a = (x^{-1}ax)a = a^{-1}a = 1$.

$\Rightarrow |xa| = 2$. But $G = \langle x, xa\rangle$ (gen. by elts of order 2, but contains an element of infinite order.

However, for nilpotent groups the situation is better.

Def Let π be ~~a~~ nonempty set of primes. A <u>π-number</u> is a positive ~~number not divisible by any prime in π~~ integer which is a product of primes of π.

An element g in a group G is a <u>π-element</u> if its order is a π-number ≥ 1

If every element of G is a π-element, then G is called a <u>π-group.</u>

(borrow the definition from p-groups, p-elements, ...).

(For a finite group G, G is a π-group $\Longleftrightarrow$ $|G|$ is a π-number (by Cauchy Thm.)).

If π is the set of all primes, then a π-element is an element of finite order. A π-group is then a torsion group. (also called periodic).

If a group has no nontrivial elements of finite order, it is called torsion-free.

<u>Theorem</u>: Let G be a nilpotent group. Then,

The elements of finite order in G form a subgroup T, called the <u>torsion subgroup</u> of G.

Also, T is fully-invariant in G ($T^{\theta} \leq T$ for all endomorphisms $\theta : G \to G$).

Moreover, G/T is torsion-free

Furthermore, T is the direct ~~product~~ sum of p-groups (for various primes p).

Pf Let π be any set of primes, and let P be the subgroup generated by all π-elements in G. Note that P is nilpotent. Also, P_{ab} is an abelian group generated by π-elements, so P_{ab} is a π-group. Apply corollary with $\mathfrak{P}$ = "be a π-group" (check it is admissible). Hence P is a π-group. So the π-elements in G ~~generate~~ form a π-subgroup..

(cont pf).

Take $\Pi = \{$all primes$\}$ - So the elements of finite order form a sgp, T.

Take $\Pi = \{p\}$. Then the p-elements form a subgroup in G, call $T_p \leq T$.

Claim: $T = \bigoplus_p T_p$

Let $g \in T$. Then $\langle g \rangle$ is finite abelian, so $\langle g \rangle$ = direct sum of p-groups.

So $g \in \bigoplus_p T_p$.

Need to show that $T_p \cap \langle T_q : q \neq p \rangle = 1$. (easy!).

Finally, G/T is torsion-free:

if $xT \in G/T$ has finite order m, then $x^m \in T$ $\therefore$ x^m has finite order $\Rightarrow x$ has f. order $\Rightarrow x \in T$.

Corollary: A finite group G is nilpotent iff it is a direct product of p-groups (for various primes p).

Pf $\Rightarrow$, by thm.

$\Leftarrow$, since p-groups are nilpotent.

Characterizations of finite nilpotent groups.

Thm Let G be a finite group. TFAE:

1) G is nilpotent.

2) Every subgroup of G is subnormal.

3) Every maximal (proper) subgroup of G is normal.

4) G is a direct product of (finite) p-groups, for various primes p.

Pf (1) $\Rightarrow$ (2): G nilpotent $\Rightarrow \exists$ a central series $1 \lhd G_0 \lhd G_1 \lhd \cdots \lhd G_c = G$, $G_{i+1}/G_i \leq Z(G/G_i)$

Let $H \leq G$. Note that $HG_i \lhd HG_{i+1}$, since $[G_{i+1}, H] \leq G_i$.

So $H = HG_0 \lhd HG_1 \lhd \cdots \lhd HG_c = G$.

Also, note that the length of H to G is $\leq$ nilpotence class of G.

(cont pf)

(2)⇒(3): Let M be a maximal in G. By hypothesis, M is subnormal in G. So $M \trianglelefteq G$ by maximality.

(3)⇒(4): Let $P \in Syl_p(G)$, and $N := N_G(P)$. If $N = G$, then $\exists$ only one $Syl_p(G)$. (if $\forall p$ this is true, then $G = \prod_{P \text{ Sylow}} P$):
Suppose $N \neq G$. $N \leq M$ a maximal subgp of G.

$$P \trianglelefteq N \leq M \trianglelefteq G$$

Let $g \in G$. Then $P^g \leq M$. P & P^g are two Sylow-p-groups in M.
By Sylow's thm., $\exists m \in M$ s.t. $P^g = P^m$. So $P^{gm^{-1}} = P$.
So $gm^{-1} \in N$. As $m^{-1} \in M$, then $g \in M \Rightarrow M = G \Rightarrow !!$

(4)⇒(1): From previous corollary //

The Fratini Subgroup.

Def Let G be any group. Define the Fratini subgroup of G, $\varphi(G)$ be the intersection of all maximal subgroups of G.
If G has no maximal subgroups (e.g $G = \mathbb{Q}^+$), define $\varphi(G) = G$.

Note that if M is maximal and $\alpha \in Aut(G)$, then M^α is maximal. So ~~M~~ $\varphi(G)$ is characteristic in G and in particular it is normal.

Def Let G be a group, $g \in G$. Then g is a non-generator of G if whenever $G = \langle g, X \rangle$, then $G = \langle X \rangle$ for any generating set X.

Theorem: For any group G, $\varphi(G)$ is the subset of (Frattini, 1884) non-generators of G.

Pf/ Spz g is a non-generator of G, and spz $g \notin \varphi(G)$. $\Rightarrow \exists M^{\leq G}_{\text{maximal}}$, $g \notin M$. Then $M \subsetneq \langle g, M \rangle = G$. But $M \neq G \Rightarrow !!$

Now, spz $g \in \varphi(G)$ but is not a non-generator. So $\exists X$ a subset of G s.t. $G = \langle g, X \rangle$, but $G \neq \langle X \rangle =: H$.

So H is proper sgp of G, and $g \notin H$.

Apply Zorn's lemma to find a 'maximal' sgp of G containing H, but not containing g, call it M. $(M \neq G)$.

Spz. $M < L \leq G$. Then $g \in L$. So L contains $\langle g, X \rangle = G$.

So M is a maximal sgp, and it does not contain $g \Rightarrow !!$ //

Theorem: If G is a finite group, then $\varphi(G)$ is nilpotent.

Pf/ Will show that all Sylow-p sgps are normal. Let $F := \varphi(G)$.

$P \in Syl_p(\varphi(G))$. Will show $P \trianglelefteq G$ (and then in particular $P \trianglelefteq \varphi(G)$).

Let $g \in G$. Then $P^g \leq \varphi(G)$ since $P \leq F \trianglelefteq G$

So P, P^g are two Sylow-p sgps. of F. By Sylow's thm, they are conjugate in F, $P^g = P^f$, $f \in F$. So $gf^{-1} \in N_G(P) =: N$. Then $g \in NF$. ($\forall g \in G$.

So $G = NF = \langle N, F \rangle$. By the non-generator property and F being finite, can omit all the elements of F (one by one) and get $G = N$. So $P \trianglelefteq G$.

//

Theorem: G a finite group. Then G is nilpotent iff $G' \leq \varphi(G)$.

Pf Let M be a maximal sgp of G.

Note that $M \trianglelefteq G \iff G' \leq M$:

($M \trianglelefteq G \Rightarrow G/M$ is cyclic of prime order $\Rightarrow G' \leq M$.

If $G' \leq M$, then $M/G' \leq G/G' = G_{ab} \Rightarrow M \trianglelefteq G$)

So $G' \leq \varphi(G) \iff G' \leq M \ \forall M$ maximal $\iff M \trianglelefteq G \ \forall$ maximal $M \iff G$ nilpotent //

- Products of Normal Nilpotent Subgroups.

Fitting's theorem: Let $H, K \trianglelefteq G$ and assume H, K are nilpotent (classes c, d) then $J := HK$ is nilpotent, with class $\leq c+d$.

Lemma: $H, K, L \trianglelefteq G$. Then, $[HK, L] = [H,L][K,L]$

$[H, KL] = [H,K][H,L]$

Pf From $[hk, l] = [h,l]^k [k,l] = [h^k, l^k][k,l]$ and so on..

Pf (of theorem): Let $J := HK \trianglelefteq G$. Will show J nilpotent by computing its LCS.

Claim: $\gamma_{i+1}(J) = \langle [L_1, \dots, L_{i+1}] : L_j = H \text{ or } K \rangle$.

Pf (by induction) on $i \geq 0$.

$i = 0$, $\gamma_1(J) = J = HK$ ✓.

$i \Rightarrow i+1$: $\gamma_{i+1}(J) = [\gamma_i(J), J] \overset{\text{Lemma}}{=} [\gamma_i(J), H][\gamma_i(J), K] \overset{\text{lemma repeatedly}}{=} \langle [L_1, \dots, L_i, H \text{ or } K], \dots \rangle$. //

Let now $i := c+d$. Then γ_{c+d+1} generated by all $[L_1, \dots, L_{c+d+1}]$, $L_i = H$ or K. In each of those commutators, there are either at least $c+1$ H's or at least $d+1$ K's.

Note that $X, Y \trianglelefteq G$ then $[X, Y] \leq X \cap Y$.

If there are $c+1$ H's, then $[L_1, \dots, L_{c+d+1}] \leq [\underbrace{H, H, \dots, H}_{c+1}] = \gamma_{c+1}(H) = 1$. //

· The Fitting subgroup.

Let G be any group. Take the subgroup generated by all the nilpotent normal subgroups of G.

Def The Fitting subgroup is $Fit(G)$, the subgroup generated by all the nilpotent normals. It need not be nilpotent, if G is infinite.

Rk: Any finite subset of $Fit(G)$ is contained in the product of finitely many nilpotent normal subgroup, which is nilpotent (by Fitting's).

Also, if G is finite, then $Fit(G)$ is nilpotent normal (and is the unique maximal such).

Example: $G = Dih(8) \times Dih(16) \times \cdots \times \overset{\text{nilpotent of class } n-1}{Dih(2^n)} \times \cdots$

Then $G = Fit(G)$, but G is not nilpotent (as the sum of classes $\to \infty$).

Reminder:

The ascending chain condition in a partially ordered set P is

if $\nexists\ p_1 < p_2 < \cdots \quad p_i \in P$.

It is equivalent to the maximal condition:

if $\emptyset \neq S \subseteq P$, then S has a maximal element (not unique, in general).

We say that a group G has the maximal condition on subgroups (Max) if $\leq(G)$ satisfies acc $\quad (\leq(G) = \{\text{subgroups of } G\})$.

Exercise: A group G satisfies max iff every subgroup of G is finitely generated.

· Finitely generated Nilpotent Groups.

Thm: Let G be a nilpotent gp. TFAE:

i) G_{ab} is finitely generated.

ii) G is finitely generated

iii) G satisfies max (all subgroups ~~satisfy max~~ are fin. generated!).

Pf (i) $\Rightarrow$ (ii) ✓(done). , and (iii) $\Rightarrow$ (i) is trivial.

(ii) $\Rightarrow$ (iii): We know that G_{ab} is fin. generated. Hence every ~~abel~~ lower central factor of G is f.g. abelian (tensor prod with G_{ab}).

Hence in the LCS,

$$1 = \gamma_{c+1}(G) < \gamma_c(G) < \cdots < \gamma_1(G) = G.$$

Each factor is f.g abelian, and so satisfies max.

Lemma: If $L \lhd K$, L & K/L have max, then K has max.

Pf/ Let $S \leq K$. Want that S f.gen.

Note $S \cap L$ is fin gen, and so is SL/L. But $\frac{SL}{L} \cong \frac{S}{S\cap L} \Rightarrow S$ fin gen. //

Example: However, $\exists$ a f.gen soluble group G, with a normal subgroup which is not finitely generated:

Let $G := \underset{\langle x\rangle}{\mathbb{Z}} \text{ wr } \underset{\langle y\rangle}{\mathbb{Z}}$. Then $G = \langle x, y\rangle$

But the base group B is the direct sum of $\overset{\text{labeled by element of } \langle y\rangle}{\infty}$ $\mathbb{Z}$'s.

B is not fin.gen, but $B \lhd G$. //

- Upper Central Series in Nilpotent Groups.

Lemma: G a gp. $x, y \in G$ s.t $[x,y] \in Z(G)$. Then, $[x^n, y] = [x, y^n] = [x,y]^n$.

Pf induction: $[x^{n+1}, y] = [x x^n, y] = [x,y]^{x^n} [x^n, y] = [x,y]\,[x^n, y] = [x,y]^{n+1}$ //

Lemma: G a gp. such that $Z(G)$ is torsion-free. Then, each factor of the upper central chain $Z_{i+1}(G)/Z_i(G)$ is also torsion-free.

Pf It is enough, by induction, to show that $Z_2(G)/Z_1(G)$ is torsion-free.

$$Z_2(G)/Z_1(G) = Z\left(G/Z_1(G)\right) = Z\left(G/Z(G)\right)$$

Suppose $z \cdot Z_1(G) \in Z_2(G)/Z_1(G)$ has finite order (n).

Then $z^n \in Z_1(G) = Z(G)$. Since $[z,g] \in Z_1(G) = Z(G)$

Hence, for $g \in G$, $1 = [z^n, g] \overset{\text{and lemma}}{=} [z,g]^n$. But $[z,g] \in Z(G)$ which is torsion free

So $[z,g] = 1 \Rightarrow z \in Z(G) \Rightarrow z\,Z_1(G) = Z_1(G)$. //

Corollary: If G is a finitely generated nilpotent group with torsion-free center, then G has a central series with each factor infinite cyclic.

Pf The U.C.S. of G has torsion-free factors (and reaches G).

Also, G satisfies max. So each subgroup of G is finitely-generated.

Hence the U.C. factors of G are fin-gen torsion-free abelian groups.

So they are free abelian of finite rank $(\cong \mathbb{Z} \oplus \overset{k}{\cdots} \oplus \mathbb{Z})$

So can refine this series so that one gets $\mathbb{Z}$ at each factor. //

Proposition: Let G be a nilpotent group.

(i) If $Z(G)$ has finite exponent dividing e (i.e. $x^e = 1 \ \forall x \in Z(G)$)., then G has finite exponent (dividing e^c, where c is the nilpotent class of G).

(ii) Assume G is finitely-generated. If G is infinite, then $Z(G)$ must have an element of infinite order.

Pf (i) First, some notation: $G^n := \langle g^n : g \in G \rangle \trianglelefteq G$. Then G/G^n has exp $| n$.

~~want to see that~~ $Z(G)^e = 1$. It is enough (by induction on c) to show that $\left(Z_2(G)/Z_1(G)\right)^e = 1$, for then $G/Z_1(G)$ has class $c-1$ (>0)

$$\left(G/Z_1(G)\right)^{e^{c-1}} = 1 \Rightarrow G^{e^{c-1}} \leq Z_1(G) \Rightarrow G^{e^c} \leq Z(G)^c = 1.$$

Let now $z \in Z_2(G)$. want that $z^e \in Z(G)$. Let $g \in G$.

$$[z^e, g] = [z, g]^e = 1 \text{ because } [z,g] \in Z(G).$$ //

(ii) By contradiction, suppose $Z(G)$ has no elements of infinite order. So $Z(G)$ is a torsion group. By max, $Z(G)$ is also finitely generated. So it is a f.g. torsion abelian gp $\Rightarrow$ $Z(G)$ is finite (of order, say m). So $Z(G)^m = 1$. Hence (by part (i)) G ~~fi~~ has finite exponent. Then G_{ab} is f.gen. with fin. exponent $\Rightarrow$ G_{ab} is finite $\Rightarrow$ G finite $\Rightarrow$!!

//

Def Let $\mathcal{P}$ be any group-theoretic property. A group G is <u>residually $\mathcal{P}$</u> if the intersection of all normal subgroups $N \trianglelefteq G$ such that G/N has $\mathcal{P}$ is 1.

__Example__: p a prime. Then $\mathbb{Z}/p^i\mathbb{Z}$ is a finite p-group, and $\bigcap_i p^i\mathbb{Z} = 0$

So $\mathbb{Z}$ is residually finite-p group.

__Prop__ (equivalent form of the definition): G is residually $\mathfrak{P} \Leftrightarrow$ given $1 \neq g \in G$,

$\exists\ N \triangleleft G$ s.t. $g \notin N$ and G/N has $\mathfrak{P}$.

Interesting properties are "finite", or "finite-p".

__Theorem__ (Gruenberg, '50): Let G be a fin. gen. torsion-free nilpotent gp. Let p be any prime. Then G is residually finite-p.

Pf Can assume $G \neq 1$. Let $C := Z(G)$, $c :=$ nilpotent class of G, $c > 0$.

Use induction on c.

Note that G/C is fin. gen, torsion-free, nilpotent of class $c-1$. Hence, G/C is residually finite-p. Let $1 \neq g \in G$ arbitrary. We'll show that $g \notin N \triangleleft G$, where G/N is finite-p group.

If $g \notin C$, then as C is normal and G/C is finite p, we're done.

So assume from now on that $g \in C$.

C is a fin. gen. torsion-free abelian gp $\Rightarrow C$ free abelian $\Rightarrow C \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$

Hence $\bigcap_i C^{p^i} = 1$. Hence $g \notin L = C^{p^i}$ for some $i \geq 1$

Choose a subgroup M maximal subject to: $\cdot\ L \leq M \triangleleft G$ (either by Zorn's or by max of G).
$\cdot\ g \notin M$

We'll show that G/M is a finite p-group, thus completing the proof.

Suppose G/M infinite (+ f.g. + nilpotent) $\overset{\text{by last prop (ii)}}{\Longrightarrow} Z(G/M)$ contains an element of infinite order.

Call it zM

__Claim__: $\langle z, M \rangle \triangleleft G$, $g \notin \langle z, M \rangle^{\text{wt}}$ ($\Rightarrow$!!)

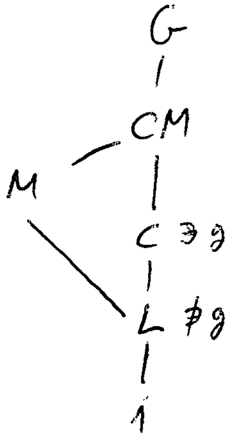
(a subgroup of $Z(G/M)$ is $\triangleleft\ G/M$). and $L \leq \langle z, M \rangle$ also!

Suppose now that $g \in \langle zM \rangle$. So $g = z^r m$, $m \in M$, $r \neq 0$.

Then $z^r = gm^{-1} \in C \cdot M$. Also, C/L is finite (C/C^{p^i} is f.gen. ab. torsion $\Rightarrow$ finite).

Hence, some power (say $z^{s \neq 0}$) is in $LM = M$.

So $|zM|$ is finite $\Rightarrow !!$



We only need to show now that G/M is a p-group (just proved it was finite).

Note that G/M is finite nilpotent. So

$G/M \cong \prod H_i$, H_i groups of prime order. Note that $p \mid |G:M|$

~~Assume that G/M~~ As C/L is a p-group, then CM/M is also.

Suppose that $\frac{G}{M} = \underbrace{\frac{P}{M}}_{}^{\text{the p-group}} \times \frac{Q}{M} \times \cdots$ want to show that $P/M = G/M$.

P/M, $Q/M \cdots$ are all normal in G/M.

Therefore, $P \trianglelefteq G$, $Q \trianglelefteq G$, $M \leq P$, $M \leq Q$.

So by maximality of M, $g \in P \cap Q = M \Rightarrow !!$ Hence G/M is a p-group.

//

Finite p-groups

These form a very complex class of groups. For example, have the following:

Thm (Higman): The number of non-isomorphic groups of order p^n is

$$p^{A(n) n^3}, \quad A(n) = \frac{2}{27} + O(n^{-1/3}).$$

$|G| = p^n$

$n=1$: G cyclic of order p.

$n=2$: G is abelian, $G \cong C_{p^2}$ or $G \cong C_p \oplus C_p$.

$\langle x \rangle \ltimes \langle a \rangle$, $x : a \mapsto a^{1+p}$

$n=3$: abelian gps: C_{p^3}, $C_{p^2} \oplus C_p$, $C_p \oplus C_p \oplus C_p$

two nonabelian types: $C_p \ltimes C_{p^2}$, $C_p \ltimes (C_p \oplus C_p)$.

action as $x \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

For $p=2, n=3$, we get $\mathrm{Dih}(8)$ and Q_8 (quaternion gp).

Burnside Basis Theorem.

Let G be a finite p-group. Then

(i) $\varphi(G) = G' \cdot G^p \quad (G^p = \langle g^p : g \in G \rangle)$.

(ii) If $|G : \varphi(G)| = p^r$ and $G = \langle X \rangle$ (for some set X), then there is a subset $Y \subseteq X$ with $\# Y = r$ s.t. $G = \langle Y \rangle$

Proof:

(i) If M is maximal in G, then $M \lhd G$ (because G is nilpotent).

Hence G/M is a group of prime order p. So $G' \leq M$ and $G^p \leq M$

So $G'G^p \leq M$. ($\forall$ maximal M). Thus $G'G^p \leq \varphi(G)$.

Look at $G/G'G^p$: it is abelian of exponent p i.e. it's a direct sum of groups of order p.

Clearly, $\varphi\left(G/G'G^p\right) = 1 \Rightarrow \varphi(G) \leq G'G^p \Rightarrow \checkmark$.

(ii) $|G/\varphi(G)| = p^r$. $G/\varphi(G)$ is an elementary abelian p-group, so it's a vectorspace $\overset{\dim r}{\text{over}}$ $GF(p)$. Call $V := G/\varphi(P)$.

Since $G = \langle X \rangle$, then $\langle x + \varphi(G) \mid x \in X \rangle = G/\varphi(G) = V$.

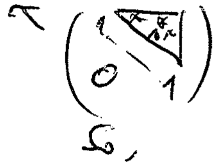
Hence $\{x + \varphi(G) \mid x \in X\}$ contains a basis $\{y + \varphi(G) : y \in Y\}$. $(|Y| = r)$.

Hence $G = \langle Y, \varphi(G) \rangle$. As $\varphi(G)$ is finite & by the non-generator property of $\varphi(G)$, we get $G = \langle Y \rangle$.

Let $d(G)$ be the minimum number of generators for a finitely-generated group.

Corollary: if G is a finite p-group and $[G : \varphi(G)] = p^r$, then
$d(G) = r$.

Example: $U_n(p) =: G$ (gp of $n \times n$ unitriangular matrices over $GF(p)$).



$\varphi(G) = G'G^p$

$G' = \{$matrices in G whose 1^{st} superdiagonal is $0\}$. So,

$|G/G'| = p^{n-1}$. In fact, $\frac{G}{G'} \simeq \underbrace{C_p \oplus \cdots \oplus C_p}_{n-1}$. Note also $G^p \leq G'$.

Thus, $\varphi(G) = G'$ and then the minimum number of generators is $n-1$. In fact, E_{ij} = elem $n \times n$ matrix with a 1 in (i,j) position (and rest 0).

Then $G = \langle 1 + E_{12}, 1 + E_{23}, \dots, 1 + E_{n-1,n} \rangle$.

§4. Soluble Groups

Def: A Chief series in a group G is a normal series

$$1 = G_0 < G_1 < \cdots < G_n = G \qquad G_i \triangleleft G$$

that does not admit any proper refinements which are normal series

There is a theory of chief series which is similar to that of composition series:

called Chief factors

(i) A normal series $1=G_0<G_1<\cdots<G_n=G$ is chief iff each G_{i+1}/G_i has no proper nontrivial G-invariant subgroups.

(ii) Two chief series in G are isomorphic (i.e. there is a bijection between the sets of factors in which corresponding factors are G-isomorphic (like a module isomorphism).)

(iii) A group G has a chief series iff the set of normal subgroups of G satisfies the a.c.c. and d.c.c.

Theorem: Let G be a finite soluble group. (due to Galois)

(i) Each chief factor of G is an elementary abelian p-group (for various primes p).

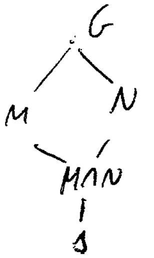
(ii) The index of a maximal subgroup of G is a power of a prime.

Pf i) Enough to show that if N is a minimal normal sgp of G, then N is an elementary abelian p-group.

Since G is soluble, so is N. Also, $N \neq 1$. We have $N' < N$, and also N' char $N \triangleleft G$. So $N' \triangleleft G$. Hence $N' = 1$ (by minimality).

This means that N is abelian. Now want that N is elementary. Let p be a prime dividing $|N|$, and write $P := \{a \in N : a^p = 1\}$. Then $P \leq N$ (N abelian!) Also $P \neq 1$ (by Cauchy's thm). Also P char N. This means $P \triangleleft G$, so $P = N$. //

(ii) Let M be a maximal subgroup of G. There is a ~~least~~ largest integer $i \geq 0$ such that $G^{(i)} \not\leq M$ (because $M \neq G$). Let $N := G^{(i)}$ $(N \not\leq M)$.
Then $N' = (G^{(i)})' = G^{(i+1)}$. Then $N' \leq M$. Also, $N' \trianglelefteq G$ $(N' \text{ char } N)$.
So M/N' is maximal in G/N'. We might assume, then, that $N' = 1$
(since $[G/N' : M/N'] = [G:M]$).
So assume N abelian.



Since $N \not\leq M$, we have $M < MN$. By maximality, $G = MN$.
Since $N \trianglelefteq G$, $M \cap N \trianglelefteq M$. Also, N abelian, so $M \cap N \trianglelefteq N$.
Since $G = MN$, then $M \cap N \trianglelefteq G$.
Once again, use that $M/M\cap N$ is maximal in $G/M\cap N$, so can assume $M \cap N = 1$.

Claim: N is minimal normal in G.

Pf Suppose $1 < L < N$ and $L \trianglelefteq G$. Note that $L \not\leq M$ (ow, $L \leq M\cap N = 1$).
Thus $G = LM$. Hence, $N = N \cap (LM)$.
The modular law says that $(N=) N \cap (LM) = L(\overset{\overset{1}{\shortparallel}}{N \cap M}) \Rightarrow N = L \Rightarrow !!$
Hence N is minimal normal in G.

By part (1), $|N| = p^r$ for some prime p, $r \geq 0$. So $|G:M| = |MN:M| = \underset{\underset{|N| = p^r}{\shortparallel}}{|N:M\cap N|}$

Supersolvable groups.

Def A group G is called supersolvable if it has a normal series with cyclic factors.

RK: For G a finite group, it is supersolvable iff each of its chief factors has prime order.

Pf $\Leftarrow$) obvious
$\Rightarrow$) refine the given normal series to a chief series (ok since G is finite). Its factors will be cyclic, and so of prime order.

Note that, for finite groups, we have:

$$\text{nilpotent} \underset{\not\Leftarrow \atop S_3}{\Longrightarrow} \text{supersoluble} \underset{\not\Leftarrow \atop A_4}{\Longrightarrow} \text{soluble}$$

Example:

- $T_n(p)$, the group of $n \times n$ triangular matrices over $GF(p)$ is supersoluble (exercise)

Theorem: if G is a supersoluble group (not necessarily finite), then G' is nilpotent.

Pf/ There's a normal series $1 = G_0 < G_1 < \dots < G_n = G$ $(G_i \trianglelefteq G)$, G_{i+1}/G_i cyclic.

If $g \in G$, conjugation by g in G_{i+1}/G_i induces an automorphism on G_{i+1}/G_i

This gives a homomorphism $\theta_i : G \longrightarrow \mathrm{Aut}(G_{i+1}/G_i)$

Let $K_i := \mathrm{Ker}(\theta_i) \trianglelefteq G$. Also $G/K_i \simeq \mathrm{Im}\,\theta_i \leq \mathrm{Aut}(G_{i+1}/G_i)$

Since G_{i+1}/G_i is cyclic, $\mathrm{Aut}(G_{i+1}/G_i)$ is abelian.

Hence G/K_i is abelian, and so $G' \leq K_i$ $(\forall i)$.

Thus $[G_{i+1}, G'] \leq G_i$ $\forall i = 0..n-1$. $[G, \underbrace{G', \dots, G'}_{n}] \leq G_0 = 1$.

So $[\underbrace{G', G', \dots, G'}_{n+1}] = 1$. Hence $\gamma_{n+1}(G') = 1$, and G' is nilpotent. //

The Schur-Zassenhaus Theorem.

Def: Let $N \trianglelefteq G$. A complement of N in G is a subgroup $H \leq G$, such that $G = HN$, and $H \cap N = 1$. (So G is a semidirect product of H, N)

We also say that G splits over N. $$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] & G \arrow[r] & G/N \arrow[r] \arrow[l, bend left] & 1 \end{tikzcd}$$

(and the two definitions are equivalent — exercise —).

Theorem: (Schur - Zassenhaus):

Let G be a finite group and $N \triangleleft G$. Assume that $\gcd(|N|, |G:N|) = 1$.

Then 1) G splits over N.

2) All complements of N in G are conjugate

Pf/ Need to show that $\exists\, H \leq G$, $H \cap N = 1$, $HN = G$.

Note that $|H| = |HN : N| = |G : N|$ since $H \cap N = 1$.

we need to find a subgroup with order $|G:N|$, and that all the subgroups of this order are conjugate.

Let $n = |N|$, $m = |G:N|$.

Case $\underline{N \text{ is abelian}}$ (Schur):

Write $Q = G/N$. Note that Q acts on N by conjugation:

$a \in N$, $g \in G$, then $a^{gN} := a^g \; (= g^{-1}ag)$. well defined <u>because N is abelian</u>.

Choose a transversal (a set of coset representatives) to N in G.

$\{t_x : x \in Q\}$ (so $x = t_x N$). Note that $|\{t_x : x \in Q\}| = |Q| = m$.

Let $x, y \in Q$. Then $xy = t_x t_y N = t_{xy} N$. So $t_x t_y = t_{xy} c(x,y)$ for some $c(x,y) \in N$.

Also, $(t_x t_y) t_z = t_x (t_y t_z) \Rightarrow (t_{xy} \cdot c(x,y)) t_z = t_x t_{yz} c(y,z) \Rightarrow$

$\Rightarrow t_{xy} t_z (t_z^{-1} \underbrace{c(x,y)}_{N} t_z) = t_{xyz}\, c(x,yz) c(y,z)$. By the action by Q on N,

have $\underbrace{t_{xy} t_z}_{t_{xyz}\, c(xy,z)} c(x,y)^z = t_{xyz}\, c(x,yz) c(y,z) \xRightarrow{\text{cancelling } t_{xyz}} c(xy,z) c(x,y)^z \underset{(*)}{=} c(x,yz) c(y,z)$

$(\forall\, x,y,z \in Q)$

(note that this is the 2-cocycle condition).

Define now, for $y \in Q$, $d(y) := \overset{\in N}{\prod_{x \in Q}} c(x,y)$ (well defined because $c(x,y) \in \overset{\text{abelian}}{N}$ so order is irrelevant

Form the product of equation (*) over all $x \in Q$, with $\cancel{y}, z$ fixed:

$$\underbrace{\prod_{x} c(xy,z)}_{\overset{\shortparallel}{d(z)}} \cdot \underbrace{\prod_{x} c(x,y)^{z}}_{\overset{\shortparallel}{d(y)^{z}}} = \Big(\underbrace{\prod_{x} c(x,yz)}_{\overset{\shortparallel}{d(yz)}}\Big)\, c(y,z)^{\overset{\swarrow \text{ Powers, not conjugation!}}{m}}$$

So we get $d(z) \cdot d(y)^{z} = d(yz) \cdot c(y,z)^{m}$. (**)

Recall that $|N| = n$ and $\gcd(m,n) = 1$. Hence, the map $\overset{N}{\overset{\downarrow}{a}} \mapsto a^{m}$ is injective. As it is $N \to N$ it is also surjective. So each element of N is a mth power.

Write $d(y)^{-1} = e(y)^{m}$ $(e(y) \in N)$.

Substituting in (**), $e(z)^{-m}\left(e(y)^{z}\right)^{-m} = e(yz)^{-m}\, c(y,z)^{m}$

So $c(x,y)^{m} = e(yz)^{m}\, e(z)^{-m}\left(e(y)^{z}\right)^{-m}$. Taking m-th roots (by bijectivity)

$c(\cancel{x},y) = e(yz)\, e(z)^{-1}\left(e(y)^{\cancel{z}}\right)^{\cancel{z}-1}$. Also, $\boxed{e(yz) = e(z)\, e(y)^{z}\, c(y,z).}$ $(\forall y,z \in Q)$

Choose now a new transversal $\{s_x : x \in Q\}$. $(s_x N = t_x N)$, as

$s_x := t_x\, e(x)$ (recall that $e(x)^{m} = d(x)^{-1}$).

<u>Claim</u>: $\{s_x : x \in Q\}$ is a subgroup:

$$s_y s_z = t_y e(y)\, t_z e(z) = t_y t_z\, e(y)^{t_z} e(z) = t_y t_z\, e(y)^{z} e(z) =$$
$$= t_{yz}\, \underbrace{c(y,z)\, e(y)^{z} e(z)}_{e(y,z)} = t_{yz}\, e(y,z) = s_{yz} \quad /\!/$$

Take now two complements H, H^{*} for N in G. We want to see that H and H^{*} are conjugate. Note that $|H| = |H^{*}| = |Q|$

Write $H = \{s_x : x \in Q\}$, $H^{*} = \{s_x^{*} : x \in Q\}$ where $x = s_x N = s_x^{*} N$.

We can write $s_x^{*} = s_x\, a(x)$, $a(x) \in N$.

Now $s_x^{*} s_y^{*} = s_{xy}^{*}$. So $s_x a(x) s_y a(y) = s_{xy} a(xy) \Rightarrow s_x s_y a(x)^{y} a(y) = s_{xy} a(xy)$

$\Rightarrow s_{xy} a(x)^{y} a(y) = s_{xy} a(xy) \Rightarrow a(x)^{y} a(y) = a(xy)$ (1-cocycle condition).

Let $b := \prod_{x \in Q} a(x) \in N$.

we get that (product over all $x \in Q$, y constant) $b = b^y a(y)^m$

Write $b = c^m$ for some $c \in N$. So $c^m = (c^m)^y a(y)^m \Rightarrow$

$\Rightarrow c = c^y a(y) \Rightarrow a(y) = c^{-y} c$.

Then, $s_y^* = s_y a(y) = s_y c^{-y} c = s_y (s_y^{-1} c^{-1} s_y) c = c^{-1} s_y c = s_y^c$.

Hence H^* and H are conjugate.

General case (N not abelian):

1) Existence of complement:

Argue by induction on $|G|$ that there is a subgroup of order $m = |G:N|$.

Let $p \mid n = |N|$ (>1, if $|N| = 1$ nothing to prove).

Let P be a Sylow p-subgroup of N. Put $L = N_G(P)$, and write $C := Z(P) \neq 1$ (P a finite p-group), $M := N_G(C)$. (Note that $L \leq M$)

~~The results holds (by induction) for G/C~~

(To see $L \leq M$, want to see that L normalizes C. As C char P and ~~the~~ ~~V~~ elements of L induce actions on P by conjugation, $Z(P)^\ell = Z(P)$ $\forall \ell \in L$:)

Apply the Frattini argument to get $G = LN$:

Let $g \in G$; Then $P, P^g \leq N$ are two Sylow p-sgps of $N (\trianglelefteq G)$.

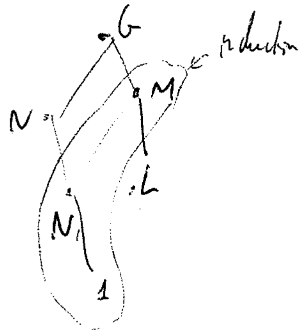
Hence $P^g = P^x$, $x \in N$ (by Sylow's thm). ∴ $P^{gx^{-1}} = P \Rightarrow gx^{-1} \in L \Rightarrow g \in LN$.

Hence $G = LN \Rightarrow G = MN$.

Let $N_1 := N \cap M \trianglelefteq M$ (because $N \trianglelefteq G$). $|N_1| \mid |N| = n$, and $[M:N_1] = |M:N \cap M| =$

$= |MN:N| = |G:N| = m$.

(cont of Schur-Zassenhaus)



Note that $\gcd\{|N_1|, |M:N_1|\} = 1$.

Apply induction to M/C with $N_1 C/C \triangleleft M/C$.

As $C \neq 1$, then $|M/C| < |G|$.

Hence M/C has a subgroup of order m, call it Y/C.

Recall that C is a p-group and $p \mid n$.

Also $|Y/C| = m$, C is a p-group and $p \nmid m$. As C is abelian, we've solved this case. So Y has a subgroup of order m, $\Rightarrow \checkmark$. //

Conjugacy of complements.

Let H, H^* be complements of N in G i.e. sgps of order m. Need to show that H, H^* are conjugate.

Case (a): N is soluble. ($N' \neq 1$) $\leftarrow$ if $N' = 1$, then N is abelian and we are done.

Thus, $N' < N$. Arguing by induction on $|G|$, can say that the result is true for G/N' ($|G/N'| < |G|$). by the abelian case.

Note that $H \cap N = 1 = H^* \cap N$. So HN'/N' and H^*N'/N' (are isomorphic to H and H^* (resp).) are complements of N/N' and G/N'. So they are conjugate (by the abelian case), i.e. $\exists g \in G : \left(HN'/N'\right)^{gN'} = H^*N'/N'$ i.e. $H^g N' = H^* N' =: T$

Now H^g, H^* are complements of N' in T. $H^g \cap N = 1 = H^* \cap N$, so because $N' \trianglelefteq N$, apply induction on N' to see that H^g and H^* are conjugate in T. $\Rightarrow H, H^*$ are conjugate in G.

Case (b): G/N is soluble.

Let π be the set of primes dividing $m = |G:N| > 1$.

Define R to be the subgroup generated by all the normal π-subgroups of G ($=: O_\pi(G)$).

&

(cont of 8-7).

Then R is the unique largest normal π-subgroup of G. Suppose $R \neq 1$.

Now $|H| = m$, so HR is a π-subgroup (not necessarily normal).

Also, $|HR:H| \mid |G:H| = |N| = n$. Therefore, $|R: H \cap R| \mid n$. Yet, $|R: H\cap R|$ is a π-number. So $R = H \cap R$, since $\gcd\{m, n\} = 1$.

Thus, $R \leq H$. In the same way, $R \leq H^*$.

So we can look at G/R, which has smaller order $(R \neq 1)$.

By induction, H/R and H^*/R are conjugate in $G/R \Rightarrow H$ and H^* are conjugate in G so ok.

If $R = 1$, then let L/N be a minimal normal subgroup of G/N.

Since G/N is soluble, L/N is an elementary abelian p-group for some prime $p \mid m$. So $p \in \pi$.

Now, $H \cap L \cong (H \cap L)N/N \leq L/N$ (because $H \cap N = 1$).

So $H \cap L$ is a p-group. $HN \geq HN = G$. So $HN = G$.

Also, $|L : H\cap L| = |HL : H| = |G:H| = n$. Thus, as $p \nmid n$, $H \cap L$ is a Sylow p-subgroup of L. The same holds for $H^* \cap L$.

Hence, Sylow's theorem implies that $H \cap L$ and $H^* \cap L$ are conjugate.

Write $H \cap L = (H^* \cap L)^g$ $(g \in L)$. $H \cap L = (H^* \cap L)^g = H^{*g} \cap L$.

Next, put $S = H \cap L = H^{*g} \cap L$. Then $S \trianglelefteq H$. Also, $S \trianglelefteq H^{*g}$ (since $L \trianglelefteq G$).

Let $J := \langle H, H^{*g} \rangle$. So $S \trianglelefteq G$.

If $J = G$, then $S \trianglelefteq G$, yet S is a p-group. As $p \in \pi$, $S \leq O_\pi(G) = R = 1$.

Then $H \cap L = 1 \Rightarrow |L| = n = |N| \Rightarrow !!$ because L was a minimal normal.

Hence, $J \neq G$, so $|J| < |G|$. By induction on $|G|$, H and H^{*g} are conjugate in J. $\therefore H, H^*$ are conjugate in G.

By Feit-Thomson theorem, a group of odd order is soluble $\Rightarrow$ whole theorem as one of $|N|$ or $|G/N|$ is odd.

Corollary: Let $N \trianglelefteq G$, $n = |N|$ and $m = |G:N|$ relatively prime.

Suppose $K \leq G$ and $|K| \mid m$. Then,

K is contained in a complement of N (i.e. in a subgroup of order m).

Pf By the S-Z theorem, $\exists\, H \leq G$ st $G = HN$, $H \cap N = 1$, $|H| = m$.

Then $KN = KN \cap HN \overset{\text{modular law}}{=} (KN \cap N)N$

Also K and $KN \cap H$ are two complements of N in KN.

Also, $|KN:N| = |K : N \cap K| = |K| \mid m$.

$\therefore \gcd\{|N|, |KN:N|\} = 1$. By the conjugacy class of S-Z, K and $KN \cap H$ are conjugate in KN.

Say $K = (KN \cap H)^x \leq H^x$ and $|H^x| = m$.

•Hall Subgroups of Finite Soluble Groups.

Let π be a set of primes, and π' the set of primes not in π.

By Zorn's lemma, every group has a maximal π-subgroup. Call this a Sylow-π-subgroup of G.

If $\pi = \{p\}$ and G is a finite group, this is consistent with usage in finite gp th.

In general, while Sylow-π-subgroups exists, they need not be conjugate, even in a finite group. However, if G is finite soluble, this is true!

Def A Hall π-Subgroup of a finite group G is a π-subgroup H s.t. $|G:H|$ is a π'-number.

Clearly, a Hall π-subgroup is a Sylow π-subgroup.

Example: Hall π-subgroups need not exist.

Let $G = A_5$. Choose $\pi = \{3, 5\}$. $\pi' = \{2, 7, \dots\}$.

Spz that H is a Hall-π-sgp. of A_5. $|H|$ is a π-number, so $3 \mid |H|$, $5 \mid |H| \Rightarrow$

$\Rightarrow |H| \geq 15 \Rightarrow |G:H| \leq 4 \Rightarrow A_5$ would embed into $S_4 \Rightarrow$!! ↯

Hence $|H|$ is not divisible by both 3 and 5.

Then $|G:H|$ is not a π'-number $\Rightarrow$ H is not Hall.

Conclusion: Hall sgps need not exist. (but observe that A_5 is non-soluble).

Also, let $K = \langle (123) \rangle$ and $L = \langle (12345) \rangle$, then K and L are Sylow π-subgroups. K, L not even isomorphic $\Rightarrow$ not conjugate.

Conclusion: don't hope for Sylow's thm on π-Sylows.

Theorem: (P. Hall, 1928). (Generalized Sylow, for solubles).

Let G be a finite soluble group, and π any nonempty set of primes. Then, every π-subgroup of G is contained in a Hall subgroup.

(in particular, they exist).

Also, any two Hall π-subgroups are conjugate.

Alternative version: G finite soluble

Assume that $|G| = mn$, $\gcd\{m, n\} = 1$.

Then there is a subgroup of order m, and any two such sgps are conjugated.

(Weak converse of Lagrange).

Equivalence of thms:

Let $\pi = \{p : p \text{ prime}, p \mid m\}$. Let H be a Hall-π-sgp. Then $|H| \mid |G| = mn$. $\Rightarrow |H| \mid m$. Then, $[G:H] = \left(\frac{m}{|H|}\right) \cdot n$. As $|G:H|$ is a π'number and $\frac{m}{|H|}$ is a π-number, must have $m = |H|$.

Pf (of 1st version):

Every π-subgroup of G is contained in a maximal π-sgp, i.e. in a Sylow π-subgroup.

We will prove that, if P is a Sylow π-sgp, then it's a Hall π-sgp.

$\downarrow$

Want to see that $|G:P|$ is a π'-number, by induction on $|G|$.

Let R be the subgroup generated by all normal π-subgroups of G,

so R is the unique maximal normal π-subgroup of G.

Then PR is a π-subgroup, containing P. As P is Sylow-π, $PR = P$,

Now, $R \leq P$.

Suppose that $R \neq 1$. Then the theorem is true for G/R (induction).

Also, P/R is a Sylow π-sgp of G/R. By induction, P/R is a Hall π-sgp of G/R.

But $|G/R : P/R| = |G:P| \Rightarrow |G:P|$ is a p'-number.

If $R = 1$, then since G is soluble ($\neq 1$), then it has a normal abelian subgroup $A \neq 1$. Now the π-primary component of A, A_π (elts of order π-numbers). A_π char $A \trianglelefteq G$. So $A_\pi \trianglelefteq G$.

Hence, as $R = 1$, $A_\pi = 1$, so A is a π'-group.

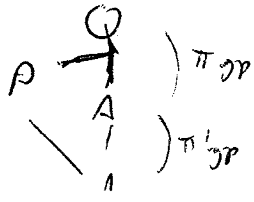
By induction, the result is true for G/A.

Hence PA/A is contained in a Hall π-subgroup of G/A, say Q/A.

So Q/A is a π-gp, with $|G:Q|$ is a π'-number.

Note that $P \cap A = 1$, so $P \cong PA/A \leq Q/A$. Thus, $|P| \,\big|\, |Q/A|$.

Apply now the corollary to S-Z thm:



Can say that P is contained in a subgroup P^* of Q,

with order $|P^*| = |Q:A|$, which is a π-number.

Since P is a Sylow π-sgp, must have $P = P^*$. Hence $|P| = |P^*| =$

$= |Q:A|$

$\therefore$, $|Q:P| = \frac{|Q|}{|Q:A|} = |A|$, which is a π'-number.

Finally, $|G:Q|$ is a π'-number. So $|G:P|$ is a π'-number $\Rightarrow$ ✓

First part.

(cont pf)

· pf that any two Hall π-sgps are conjugate.

Let P_1, P_2 be two Hall π-sgps of G.

As in (1), we can assume that G has no nontrivial normal π-sgps.

(by using induction on $|G|$).

Let A be a nontrivial abelian normal sgp of G. By induction on $|G|$, the theorem is true by G/A.

Next, P_1A/A and P_2A/A are Hall π-sgps of G/A. Clearly, these are π-sgps

$|G/A : P_iA/A| = |G : P_iA| \mid |G : P_i|$ which is a π'-number.

So $|G/A : P_iA/A|$ π'. So P_iA/A is conjugate of P_2A/A (in G/A)

$\therefore$ $P_1A = (P_2A)^g$ for some $g \in G$. $\Rightarrow$ $P_1A = P_2^gA$.

P_1, P_2^g are complements of A in P_i. so apply SZ-th get P_1, P_2 conjugate.

This is a sort of converse to Hall's theorem:

Thm: Let G be a finite group which has a Hall p'-subgroup for each prime p dividing $|G|$. Then G is soluble.

The proof uses the Burnside p-q-theorem:

(Thm: Any group of order $p^m q^n$ (p, q primes) is soluble.
(use character theory, otherwise it is a hard proof).)

Note: Let $H, K \leq G$ finite.

a) $|G : H \cap K| \leq |G : H| \cdot |G : K|$.

b) if $|G : H|$ and $|G : K|$ are relatively prime, then $|G : H \cap K| = |G : H||G : K|$

Pf (of thm):

Step 1: Reduce to the case where G is simple:

Suppose $1 \neq N \trianglelefteq G$. Check hypothesis for N and G/N.

Let H be a Hall p'-sgp of G.

Then $H \cap N$ and HN/N are Hall p'-sgps of N, resp. G/N:

It is clear that they are p'-groups.

Also, $|N : H\cap N| = |HN : H| \mid |G:H| =$ a power of $p \Rightarrow$ ✓.

Similarly, $|G/N : HN/N| = |G : HN| \mid |G:H|$ $\Rightarrow$ ✓.

Hence, by induction on $|G|$, would have that N and (so) G/N soluble $\Rightarrow$ ✓.

Step 2:

Let $|G| = p_1^{e_1} \cdots p_k^{e_k}$ (p_i distinct, $e_i > 0$). We can assume $k > 2$ by Burnside p-q theorem.

Let G_i be a Hall p_i'-sgp of G.

Hence, $|G_i|$ is not divisible by p_i, and $|G : G_i|$ is a power of p_i.

So $|G:G_i| = p_i^{e_i}$ $\quad (|G| = |G_i| \cdot |G:G_i|)$.

Let $H = G_3 \cap \cdots \cap G_k$. We can see that $|G:H| = \prod_{i=3}^{k} |G:G_i| = p_3^{e_3} \cdots p_k^{e_k}$

Hence $|H| = p_1^{e_1} p_2^{e_2}$, $\Rightarrow H$ is soluble (by Burnside p-q).

Choose a minimal normal subgroup of H, say M.

Because H is soluble, M will be elementary abelian, suppose p_1-group.

Note that $|G : H \cap G_2| = |G:H| \cdot |G:G_2| = p_2^{e_2} \cdots p_k^{e_k}$.

$\therefore |H \cap G_2| = p_1^{e_1}$ $\therefore H \cap G_2$ is a Sylow p_1-sgp of G and hence of H.

Now, $M \trianglelefteq H$ and it is a p_1-subgroup. So $M_1(H\cap G_2)$ is a p_1-gp.

So $M_1(H \cap G_2) = H \cap G_2 \Rightarrow M \leq H \cap G_2 \Rightarrow M \leq G_2$

In the same way, $|H \cap G_1| = p_2^{e_2}$, so $(H \cap G_1) \cap H_2 = 1$,

and $|(H \cap G_1)G_2| = |H \cap G_1| \cdot |G_2| = p_2^{e_2}(p_1^{e_1} p_3^{e_3} \cdots p_k^{e_k}) = |G| \Rightarrow (H \cap G_1) G_2 = G$.

$\downarrow$

Therefore,

$1 \neq M^G = M^{(H \cap G_1)G_2} = M^{G_2}$ (since $M \trianglelefteq H$) $\leq G_2 < G$.

Hence G is not simple $\Rightarrow$!! //

Reference: Doerk & Hawkes, "Finite Soluble Groups".

Application:

Let G be a soluble group of order $4m$, where $2 \nmid m$, $3 \nmid m$. Then G has a normal subgroup of order m:

Pf Let H be a Hall $2'$-subgroup. $\therefore |G:H| = 4$, $|H| = m$.

G acts on the set of cosets of H, so get $\theta : G \to S_4$. Let $K := \operatorname{Ker} \theta \leq H$. $G/K \simeq$ a subgroup of S_4. Also, $4 \mid |G/K|$, $8 \nmid |G/K|$, and $3 \mid |G/K| \Rightarrow |G/K| = 4 = |G/H| \Rightarrow H \trianglelefteq G$ //

• Infinite soluble groups.

There are many different types of infinite soluble groups. The most important is the class of polycyclic groups.

Def Let $\mathcal{P}$ be some group-theoretic property. A group G is a poly-$\mathcal{P}$ group if $\exists$ series $1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ where each G_{i+1}/G_i has $\mathcal{P}$.

For $\mathcal{P}$ = "cyclic", we have the polycyclic groups.

Examples:
- all finite soluble groups are polycyclic.
- all finite generated nilpotent group is polycyclic.
- all supersoluble groups are polycyclic

$$\text{fin. gen. nilpotent} \underset{\substack{\not\Leftarrow \\ (\mathrm{Dih}(\infty)).}}{\Longrightarrow} \text{supersoluble} \underset{\substack{\not\Leftarrow \\ (A_4)}}{\Longrightarrow} \text{polycyclic}$$

Theorem: A soluble group G satisfies max iff it is polycyclic.

Pf/ Clearly, cyclic groups satisfy max. Also, max is extension-closed, so ok.

Conversely, if G is soluble with max, then all subgroups of G are finitely generated.

Hence, $G^{(i)}/G^{(i+1)}$ is finitely-generated and abelian, hence $G^{(i)}/G^{(i+1)}$ is a direct product of finitely-many cyclic groups, so can refine the series to get a polycyclic one. //

Here there is another reason why polycyclic groups are important:

1) A soluble subgroup of $GL_n(\mathbb{Z})$ is polycyclic (Mal'cev).

2/ Every polycyclic groups is isomorphic to a soluble subgroup of some $GL_n(\mathbb{Z})$. (Auslander - Swan),

Def/ The Hirsch number $h(G)$ of a polycyclic group G is the number of infinite factors in a series with cyclic factors in G (it is well defined by HW 1).
(note $h(G)=0 \iff G$ finite).

Theorem: Let G be a polycyclic group. Then, there is a normal subgroup N with finite index in G, s.t. N is poly-$\mathbb{Z}$, (So N is torsion-free).

Pf/ Let $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ be a series with cyclic factors.

If $n \leq 1$, G is cyclic and so the theorem is trivial.

Use induction on n.

Write $N := G_{n-1}$. The theorem is true for N (by induction), so

$\exists\, M \trianglelefteq N$ s.t. N/M is finite, of order m, and M is poly-infinite cyclic. Note that $N^m \leq M$. N^m is also poly-$\mathbb{Z}$, because poly-$\mathbb{Z}$ is inherited by subgroups (check, easy).

Also, N/N^m is finite (since poly-$\mathbb{Z}$ & torsion).

Finally, N^m char N, so $N^m \trianglelefteq G$. So by replacing M by N^m, we can assume that $M \trianglelefteq G$.

$$\begin{tikzcd}
G \arrow[d, dash, "\text{cyclic}"] \\
N \arrow[d, dash, "\text{finite}"] \\
M \arrow[d, dash, "\text{poly-}\mathbb{Z}"] \\
1
\end{tikzcd}$$

If G/N is finite, then G/M is finite and so we are done.

So assume G/N is infinite cyclic, $\frac{G}{N} = \langle xN \rangle$

So $G = \langle x, N \rangle$ and $\langle x \rangle \cap N = 1$.

Since N/M is finite then $\mathrm{Aut}(N/M)$ is finite. Hence, some x^r $(r > 0)$ acts trivially by conjugation on N/M.

Put $L := \langle x^r, M \rangle$. Then, $L \trianglelefteq \langle x, N \rangle = G$,

since $[N, x^r] \leq M$.

finite since $N^m = M \leq L$

Claim: L is poly-$\mathbb{Z}$ and G/L is finite.

finite because $x^r \in L$.

$\rightarrow$ G/L is finite, because $G/L = \left(NL/L\right) \cdot \left(\langle x, L \rangle / L\right)$

$\rightarrow$ $L/M = \langle x^r \rangle M/M \cong \langle x^r \rangle / \langle x^r \rangle \cap M = \langle x^r \rangle \cong \mathbb{Z}$ and M is poly-$\mathbb{Z}$ ✓.

Corollary: If G is an infinite polycyclic, then G has a non-trivial normal (finitely-generated) free abelian subgroup.

Pf By the Theorem, $\exists\, N \trianglelefteq G$ with G/N finite and N torsion-free.
As G is infinite, $N \neq 1$.
If $d :=$ derived length of N, then put $A := N^{(d-1)}$ ← derived.
A is abelian (as $A' = N^{(d)} = 1$), it is torsion free because $A \leq N$, and is finitely-generated, so it is free abelian. //.

Theorem (Mal'cev): Let G be a polycyclic group, and $H \leq G$. Then H is the intersection of some subgroups of finite index in G.

Pf If G is abelian, then $H \trianglelefteq G$ and G/H is residually finite (because it is a fin-gen abelian group).
So H is the intersection of sgps of finite index in G.
In the general case, let $l := h(G)$ (# of infinite factors of the poly-series).
If $l = 0$, G is finite $\Rightarrow$ clear. For $l > 0$, by induction:
As G is infinite ($l > 0$), then $\exists\, 1 \neq A \trianglelefteq G$ with A (torsion) free abelian.
It is easy to see that $h(G) = h(A) + h(G/A)$, and $h(A) > 0$.
So $h(G/A) < h(G) = l$, so by induction, the result is true for G/A.
Now, let $g \in G \setminus H$. We need to prove that $\exists$ a subgroup $K \leq G$ with $H \leq K$, K of finite index, and $g \notin K$.
Since the result is true for G/A, then we can assume $g \in HA$ (if $g \notin HA$, $gA \notin HA/A$ and the result follows by induction).
Write $g = ha$, $h \in H$, $a \in A$. Here $a \notin H \cap A$, $a \in A$. Can apply the result to the abelian group A.
Hence $\exists$ a subgroup B s.t. $H \cap A \leq B \leq A$, A/B finite and $a \notin B$. If $|A/B| = n$, then $A^n \leq B$, A/A^n is finite, and A^n char $A \Rightarrow A^n \trianglelefteq G$.

Now, $h(G/A^m) = h(G/A) + \cancel{h\left(A/A^m\right)}^{=0} = h(G/A)$.

Hence, the result is true for G/A^m, with the subgroup HA^m/A^m.

Now, if $g \notin HA^m$ we are done.

If in fact $g \in MA^m$, write $g = h_1 b$, $h_1 \in H$, $b \in A^m$.

As also $g = ha$, we get $ha = h_1 b$, so $ab^{-1} = h^{-1}h_1 \in H \cap A \leq B$

But as $a \notin B$ and $b \in B$, this is a contradiction. //

<u>Corollary</u>: If G is polycyclic, then it is residually finite (case $H=1$), (it is due to Hirsch).

<u>Digression</u>: Let G be a polycyclic group, and write $\mathcal{F}$ to be the set of all subgroups of finite index in G.

Put a topology on G by making $\mathcal{F}$ a base of neighborhoods of the identity.

Since G is residually-finite, this topology is Hausdorff.

If $x \neq y \in G$, then $x^{-1}y \neq 1$ and hence $\exists H \leq G$, $|G:H| < \infty$, s.t. $x^{-1}y \notin H$, so $xH \neq yH$, so these two open sets separate x and y.

Also by Malcev's theorem, every subgroup of G is closed.

To compactify G, we need to take the inverse limit.

$$G \hookrightarrow \varprojlim_{\substack{N \trianglelefteq G \\ |G:N| < \infty}} (G/N) \text{ is a profinite soluble group.}$$

Theorem (Hirsch): Let G ~~be~~ a polycyclic group, not nilpotent.

Then, some finite quotient of G is not nilpotent.

Pf/ Assume all finite quotients of G, but not G itself, are nilpotent.

Then, G must be infinite, so $h(G) > 0$.

Assume that G is a counterexample with smallest $h(G)$.

Then, $\exists\ 1 \neq A \trianglelefteq G$, with A free abelian.

Let p be any prime. Then, $A^p \trianglelefteq G$.

Now, $h(G/A^p) = h(G/A) + \cancel{h(A/A^p)}^{=0} \leftarrow A/A^p < \infty$.
$= h(G/A) < h(G)$.

G/A^p satisfies the hypothesis on G. By minimality of $h(G)$, G/A^p is nilpotent, say of class m.

Then, $[A, G, \overset{m}{\ldots}, G] \leq A^p$. $A \geq [A,G]A^p \geq [A,G,G]A^p \geq \cdots \geq [A, G \overset{m}{-} G]A^p = A^p$.

Denote $r := h(A)$, so $r = rk_{\mathbb{Z}}(A)$.

Hence A/A^p, is a $\mathbb{Z}/p\mathbb{Z}$-vectorspace, of dimension $= r$.

The subgroups $[A, G, .., G]A^p/A^p$ form a chain of subspaces.

By dimension, its length is at most r.

Hence, $[A, G, \overset{r}{\ldots}, G] \leq A^p$, $\forall p$.

$\therefore\ [A, G, \overset{r}{\ldots}, G] \leq \bigcap_p A^p = 1$ (A a free abelian group).

But G/A is nilpotent, so G is nilpotent $\Rightarrow$!!

Theorem: If G is a polycyclic group, then $\varphi(G)$ is nilpotent.

Pf/ Write $F = \varphi(G)$, which is polycyclic. Assume that F is not nilpotent. By the previous theorem, $\exists N \trianglelefteq F$, s.t. F/N finite and not nilpotent. If $m := |F/N|$, replace note that $F^m \leq N$, and F/F^m is finite. Furthermore, $F^m \trianglelefteq G$. F/F^m is not nilpotent (because F/N is not). So we assume that $N \trianglelefteq G$ (replace it by F^n).

Note also that $\varphi(G/N) = \varphi(G)/N = F/N$ (maximal of $G/N \Leftrightarrow M/N$, where M maximal in G)

We now have that $\varphi(G/N) = F/N$ is finite.

The proof for finite gps shows that a finite Frattini sgp is always nilpotent (exercise).

$\therefore$ F/N is nilpotent $\rightarrow$!!

//

Theorem: If every maximal subgroup of a polycyclic group G is normal, then G is nilpotent.

Pf/ If G is not nilpotent, then G has a finite non-nilpotent finite quotient G/N. But the max. subgroups of G/N are clearly normal. By the finite case, G/N is nilpotent

//

Remarks: (repeat some previous ones).

1) If G is a soluble subgroup of $GL_n(\mathbb{Z})$, then G is polycyclic (Mal'cev).

2) If G is any polycyclic group, then G is isomorphic to a subgroup of $GL_n(\mathbb{Z})$ (some n). (Auslander – Swan)

3) Let K be an alg. number field. Let R be its subring of algebraic integers. Then $A = R^+$ is free abelian & finitely-generated. Let $\mathcal{U}$ denote the group of algebraic units ($R^\times$). We can regard A as $\mathbb{Z}\mathcal{U}$-module, by (field) multiplication. $\therefore$ $\mathcal{U} \simeq$ a group of automorphisms of A. Let $G := \mathcal{U} \ltimes A$.

Dirichlet Units Theorem: $\mathcal{U}$ is fin. generated. Hence G is polycyclic.

§5. The Transfer.

Let G be a group, and let $H \leq G$ a subgroup with finite index, $|G:H| = n$. Choose a right transversal to H in G, $\{t_1, \dots, t_n\}$.

Then, for $x \in G$, $(Ht_i)x = Ht_{(i)x}$, where $i \longmapsto (i)x$ is a permutation of $\{1, \dots, n\}$.

Then $Ht_i x = Ht_{(i)x}$, and hence $t_i x t_{(i)x}^{-1} \in H$.

Now, assume that we have a homomorphism $\theta : H \longrightarrow A$ (A any abelian group).

Def The <u>transfer</u> of θ is the <u>map</u> $\theta^* : G \longrightarrow A$, that sends, for $x \in G$, to

$$x^{\theta^*} := \prod_{i=1}^{n} \left(t_i x t_{(i)x}^{-1} \right)^{\theta} \quad \text{(order doesn't matter, as } A \text{ is abelian).}$$

<u>Theorem</u>: The map $\theta^* : G \to A$ is independent of the choice of transversal, and it is a homomorphism.

Pf/ Take another transversal $\{t_1', \dots, t_n'\}$, and label it so that $Ht_i = Ht_i'$.

Then $t_i' = h_i t_i$ $(h_i \in H)$.

$$\prod_{i=1}^{n} \left(t_i' x t_{(i)x}'^{-1} \right)^{\theta} = \prod_{i=1}^{n} \left(h_i t_i x (h_{(i)x} t_{(i)x})^{-1} \right)^{\theta} = \prod_{i=1}^{n} h_i^{\theta} \left(t_i x t_{(i)x}^{-1} \right)^{\theta} \left(h_{(i)x}^{-1} \right)^{\theta} =$$

$$= \prod_{i=1}^{n} \left(t_i x t_{(i)x}^{-1} \right)^{\theta} \cdot \cancelto{1}{\prod_{i=1}^{n} h_i^{\theta} \left(h_{(i)x}^{\theta} \right)^{-1}} \quad . \checkmark .$$

Now, let $x, y \in G$.

$$(xy)^{\theta^*} = \prod_{i=1}^{n} \left(t_i x y t_{(i)xy}^{-1} \right)^{\theta} = \prod_{i=1}^{n} \left(\left(t_i x t_{(i)x}^{-1} \right) \left(t_{(i)x} y t_{((i)x)y}^{-1} \right) \right)^{\theta} =$$

$$= x^{\theta^*} y^{\theta^*} .$$

//

<u>Remark</u>: let $H \leq G$, A abelian. Can consider $\mathrm{Hom}(H, A)$, $\mathrm{Hom}(G, A)$, which are abelian groups, where $x^{\alpha + \beta} = x^{\alpha} x^{\beta}$ $(x \in H \text{ or } G)$.

Can define the restriction map:

$$\text{res}: \text{Hom}(G,A) \to \text{Hom}(H,A) \qquad \text{is a gp. homomorphism.}$$

$$\theta \longmapsto \theta_{|H}$$

If $|G:H| = n < \infty$, then we can define the corestriction:

$$\text{Cor}: \text{Hom}(H,A) \to \text{Hom}(G,A).$$

$$\theta \longmapsto \theta^* \quad (\text{the transfer of } \theta).$$

This maps are not inverses, but we will show that they are closely related:

First, we make some computational simplifications.

Computing the Transfer.

We'll be using the same notation (G, H, A, θ)

Let $x \in G$. Want to compute $x\theta^*$. We choose a convenient transversal to find x^{θ^*}.

When x acts on the set of cosets of H, the $\langle x\rangle$-orbits of cosets are of the form (for $i = 1..k$).

$\{Hs_i, Hs_ix, \ldots, Hs_ix^{l_i-1}\}$, where l_i is the least positive integer s.t $Hs_ix^{l_i} = Hs_i$

Note that $\sum_{i=1}^{k} l_i = n$

Clearly, $\{s_i, s_ix, \ldots, s_ix^{l_i-1}\}_{i=1..k}$ form a right transversal to H in G.

We'll use this transversal to compute x^{θ^*}, by computing the contribution to each orbit:

$$(s_ix(s_ix)^{-1})^\theta \cdot (s_ix \cdot x \cdot (s_ix^2)^{-1})^\theta \cdot \ldots \cdot (s_ix^{l_i-1} \cdot x\, s_i^{-1})^\theta = (s_ix^{l_i}s_i^{-1})^\theta.$$

Hence, $x^{\theta^*} = \prod_{i=1}^{k} (s_ix^{l_i}s_i^{-1})^\theta$;

Theorem: Let $x \in G$ and let the $\langle x\rangle$-orbits of right cosets of H (in G) be $\{Hs_i, Hs_ix, \ldots, Hs_ix^{l_i-1}\}$, $i = 1..k$. Then

$$x\theta^* = \prod_{i=1}^{k} (s_ix^{l_i}s_i^{-1})^\theta.$$

Corollary 1: Given $H \leq G$, $|G:H| = n < \infty$. Then: (!!notation of composition is twisted !!).

(cor after res)

$\text{res} \circ \text{cor} : \text{Hom}(G, A) \longrightarrow \text{Hom}(G, A)$

is multiplication by n in A.

Pf/ Let $\theta \in \text{Hom}(G, A)$. Apply res∘cor, and have to get $n \cdot \theta$.

$(\theta)\text{res} \circ \text{cor} = (\theta|_H)^*$. Let $x \in G$. Want to calculate (notation as in the thm)

$$x^{(\theta|_H)^*} = \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1})^{\theta|_H} = \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1})^{\theta} = \prod_{i=1}^{k} (s_i^{\theta} (x^{l_i})^{\theta} (s_i^{-1})^{\theta}) =$$

$$= \prod_{i=1}^{k} x^{l_i} = x^n.$$

Corollary 2: If $a \mapsto na$ is an automorphism of A (e.g. A finite and $(|A|, n) = 1$),

then $\text{res} : \text{Hom}(G, A) \to \text{Hom}(H, A)$ is injective, and

$\text{cor} : \text{Hom}(H, A) \to \text{Hom}(G, A)$ is surjective.

Transfer into a Subgroup:

Let $H \leq G$ with $|G:H| = n < \infty$. Choose $A := H_{ab}$ $(= H/H')$, and let $\nu : H \to H_{ab}$ be the canonical projection, $h^{\nu} = hH'$. Apply the transfer to ν, and get the transfer of G into H, written $\tau_{G,H}$ $(= \nu^*)$, which is a homomorphism $\tau_{G,H} : G \to H_{ab}$.

$$x^{\tau_{G,H}} = \prod_{i=1}^{n} (t_i x t_{(i)x}^{-1}) H' \quad \text{, for a general transversal } \{t_1, \ldots, t_n\}.$$

Example: transfer into the center.

Assume $H \leq Z(G)$, $|G:H| = n < \infty$. We'll find the transfer: Let $x \in G$, and use the special form for the transversal.

$$x^{\tau_{G,H}} = \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1}) \underbrace{H'}_{1} = \prod_{i=1}^{k} \overbrace{s_i x^{l_i} s_i^{-1}}^{\in H \leq Z(G) \Rightarrow x^{l_i} \in Z(G)} = x^n$$

We will state this as a theorem.

Theorem (Schur): Let G be a group, $H \leq Z(G)$, $|G:H| = n$.

Then $\tau_{G,H}$ is just $x \mapsto x^n$. Hence $x \mapsto x^n$ is an homomorphism. (in particular, $(xy)^n = x^n y^n$).

Pf //

Application (Thm. by Schur, also):

Let G be a group s.t. $|G : Z(G)| = n < \infty$. Then G' is finite and $(G')^n = 1$.

Lemma: Let H be a subgroup with finite index in a finitely-generated group G. Then H is finitely-generated.

Pf (will see it as a special case of a more general theorem, here there's an elementary pf).

Let $G = \langle X \rangle$, where X is finite, and let $\{t_1, \dots, t_n\}$ be a right transversal to H in G. Assume that $t_1 = 1$.

Then $Ht_j g = Ht_{(j)g}$ where $j \mapsto (j)g$ is a permutation of $\{1, \dots, n\}$.

We have $t_j g = h(j,g)\, t_{(j)g}$, $h(j,g) \in H$.

Let $a \in H$. We can write it as $a = y_1 \cdots y_r$, $y_i \in (X \cup X^{-1})$.

Then $a = t_1 a = (t_1 y_1). y_2 \cdots y_n = h(1, y_1)\, t_{(1)y_1} y_2 \cdots y_r = \dots$

$= h(1,y_1)\, h((1)y_1, (1)y_1 y_2) \cdots (h(\dots))$.

So a is expressed as a product of $h(1,y_1)\, h((1)y_1, y_2) \cdots h((1)y_1, (1)a)\, t_{(1)a}$

But $t_{(1)a} = t_1 = 1$ (because $a \in H$).

So H is generated by all $h(j, y)$: $j = 1, 2, \dots, n$, $y \in X$ (a finite set) //

With this theorem, we can now prove the Theorem (Schur's 2nd thm).

Pf (Schur, G' finite and $(G')^n=1$)

Put $C := Z(G)$, so $|G:C| = n$. Let $\{t_1, \dots, t_n\}$ be a right transversal to C.

Every commutator has the form $[c_1 t_{i_1}, c_2 t_{i_2}]$, $c_1, c_2 \in C$, $1 \leq i_1, i_2 \leq n$.

But $[c_1 t_{i_1}, c_2 t_{i_2}] = [t_{i_1}, t_{i_2}]$ since $c_i \in C$.

Hence, G' is finitely-generated.

Also, $G'/G' \cap C \simeq G'C/C \leq G/C$ which is finite. So $G'/G' \cap C$ is finite.

By the lemma, $G' \cap C$ is finitely-generated. It is also abelian,

Also, $x \mapsto x^n$ is a hom. $\theta: G \to C$. Hence $(G')^\theta = (G\theta)' = 1$.

Hence, $G' \leq \operatorname{Ker} \theta$, and therefore $(G')^n = 1$. Hence $(G' \cap C)^n = 1$.

As $G' \cap C$ is f.gen abelian and torsion, it is finite.

Because $G'/G' \cap C$ is finite, we get that G' is finite. //

- Transfer into a Sylow p-Subgroup.

Theorem: Let G be a finite group. Let P be a Sylow p-Subgroup (for some p).

Form the transfer $\tau = \tau_{G,P} : G \longrightarrow P_{ab}$ ~~and write $N = N_G(P)$~~. Then,

i) $\operatorname{Ker}(\tau) = G'(p) = \bigcap\limits_{\substack{N \trianglelefteq G \\ G/N \text{ is an abelian } p\text{-gp.}}} N$ (note $G/G'(p)$ is the "largest" abelian p-quotient of G).

ii) $\operatorname{Ker}(\tau|_P) = P \cap G'$.

ii) $\operatorname{Im}(\tau) = \operatorname{Im}(\tau|_P) \simeq G/G'(p)$.

Pf of Thm:

$G/\ker\tau \cong \operatorname{Im}\tau \leq P_{ab}$ = abelian p-group.

By definition of $G'(p)$, then $G'(p) \leq \ker\tau$.

Let $x \in G$. We'll use the usual transversal to P in G, arising from the $\langle x\rangle$-orbits of right cosets. ; $\{s_i, s_i x, \dots, s_i x^{l_i - 1}\}_{i=1..k}$.

$x^\tau = \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1}) P'$. Note that $PG'(p)/G'(p)$ is a Sylow p-sgp of $G/G'(p)$

Hence, as $G/G'(p)$ is a p-gp, $G = PG'(p)$. Hence can choose the s_i to belong to $G'(p)$.

Write $x^\tau = P' x^{\sum l_i} c$, where $c \in G'(p)$, because $[x^{l_i}, s_j] \in G'(p) \trianglelefteq G$

As $\sum l_i = n$, get $x^\tau = P' x^n c$

If $x \in \ker\tau$, then $P' x^n c = P'$, i.e. $x^n c \in P' \leq G'(p)$.

As $c \in G'(p)$, then $x^n \in G'(p)$.

But $G/G'(p)$ is a p-group, and $n = |G:P|$ is prime to p.

Hence $x \in G'(p)$. So $\ker\tau \leq G'(p)$, hence $\ker\tau = G'(p)$.

(i): $\ker(\tau|_P) = P \cap \ker\tau = P \cap G'(p)$

$$\begin{tikzcd} G \arrow[d, dash, "p\text{-gp}"'] \\ G'(p) \arrow[d, dash, "p'\text{-gp}"'] \\ G' \end{tikzcd}$$

So $P \cap G'(p) = P \cap G'$. //

check this!

(ii) is an application of the first isomorphism theorem, $G/G'(p) \cong \operatorname{Im}\tau$

and also $\operatorname{Im}(\tau|_P) \cong P/\ker\tau|_P = P/P\cap G' \cong PG'/G' \cong G/G'$ //

- Groups with an abelian Sylow p-subgroup.

Theorem: Let G be a finite group with an abelian Sylow p-Sgp (for a particular prime p). Put $N = N_G(P)$, and let $\tau : G \to P (= P_{ab})$ be the transfer of G into P. Then:

i) $Im(\tau) = C_P(N)$: (elements of P that are in the center of $N_G(P)$). $= P \cap Z(N)$

ii) $P \cap \ker \tau = [P, N]$.

iii) $P = C_P(N) \times [P, N]$

Rk If P is a cyclic group, then $C_P(N) = 1$ or $[P,N] = 1$!

Pf: Recall that $\operatorname{im} \tau = \operatorname{im} \tau_{|P}$.

Let $x \in P$, and use the usual transversal arising from $\langle x \rangle$-orbits of right cosets of P.

So $x^\tau = \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1})$, $\sum l_i = |G:P| =: n$.

Let $y := x^{l_i}$. Then $y \in P$, and $y^{s_i^{-1}} \in P$ $(y^{s_i^{-1}} = s_i x^{l_i} s_i^{-1})$.

Hence, if $C := C_G(y^{s_i^{-1}})$, then $C \geq \langle P, P^{s_i^{-1}} \rangle$, since P is abelian

By Sylow's theorem, $P^{s_i^{-1}} = P^c$, where $c \in C$. Then $r_i := s_i^{-1} c^{-1} \in N$.

Also, $y^{r_i} = (y^{s_i^{-1}})^{c^{-1}} = y^{s_i^{-1}}$.

So $x^\tau = \prod_{i=1}^{k} (x^{l_i})^{r_i}$ (where $r_i \in N$). $= x^{\sum l_i} \cdot d$, where $d = \prod [\overset{P}{x^{l_i}}, \overset{N}{r_i}]$

$\therefore$ $x^\tau = x^n d$, where $d \in [P, N]$.

Hence $x^n = x^\tau d^{-1} \in P^\tau [P,N]$ $\forall x \in P$.

As x is a p-element and $p \nmid n$, so $x^n \in P^\tau [P,N] \Rightarrow x \in P^\tau [P,N]$

So $P = P^\tau [P,N]$.

Suppose $x \in P$, and assume that $x^\tau \in \ker \tau$. So $1 = (x^\tau)^\tau = (x^n d)^\tau =$

$= (x^\tau)^n d^\tau = (x^\tau)^n$ (since $[P, N] \leq G' \leq \ker \tau$).

Then, $x^\tau = 1$ (as $p \nmid n$). So $\operatorname{im} \tau \cap \ker \tau = \{1\}$.

↓

Since $[P,N] \leq \ker \tau$, we get that $P = P^{\tau} \times [P,N]$

Next, $P^{\tau} \trianglelefteq N$ $\quad (N = N_G(P))$, For if $x \in P$, $g \in N$, $(x^{\tau})^g = \left(\prod_{i=1}^{n} (t_i x t_{(i)x}^{-1})\right)^g =$

$$= \prod_{i=1}^{n} t_i^g x^g (t_{(i)x}^g)^{-1}$$

As we can use the transversal $\{t_i^g : i = 1..n\}$ to P in G, (Because $g \in N$, so $G = \bigcup P t_i \Rightarrow G = G^g = \bigcup P t_i^g$). So $(x^{\tau})^g = (x^g)^{\tau}$.

Hence,

$[\operatorname{im} \tau, N] = [P^{\tau}, N] \leq P^{\tau} \cap [P,N] = 1$. So $\operatorname{im} \tau = P^{\tau} \leq C_P(N) =: C$.

We also want to see that $C \leq P^{\tau}$.

Let $x \in C$. Then $x^{\tau} = \prod_{i=1}^{k} (x^{l_i})^{r_i}$, $r_i \in N$. As $x \in C$, $x^{\tau} = \prod x^{l_i} = x^n$

$\therefore x^n \in \operatorname{im} \tau$. As $p \nmid n$, $x \in \operatorname{im} \tau$.

This proves (iii) and half of pt (i). The second part of (i) is obvious.

Finally, $[P,N] \leq P \cap \ker \tau$. Also, $|P : P \cap \ker \tau| = |\operatorname{im} P| = |P^{\tau}|$.

As we know that $P = P^{\tau} \times [P,N]$, $|P^{\tau}| = |P : [P,N]|$.

As both subgroups have the same index, $[P,N] = P \cap \ker \tau$. //

<u>Corollary</u>: Assume that G is a <u>finite group</u> with <u>all</u> of its Sylow subgroups abelian. Then $G' \cap Z(G) = 1$.

Pf/ Let P be a Sylow p-subgroup of G, $(G' \cap Z(G)) \cap P \leq P \cap \ker \tau$

By the theorem, $P \cap \ker \tau = [P,N]$.

On the other hand, $(G' \cap Z(G)) \cap P \leq C_P(N)$. $\Big\}$ As $[P,N] \cap C_P(N) = 1$,

Hence $(G' \cap Z(G)) \cap P = 1$. $\forall P \Rightarrow G' \cap Z(G) = 1$. //

<u>Rk</u>: The groups with all Sylow sgps abelian are called A-groups. There are some complicated such A-groups...

• Burnside's Criterion for Non-simplicity.

Thm Let G be a finite group, and let P be a Sylow p-Subgroup. Assume that $P \leqslant Z(N_G(P))$. Then, there is a normal p'-subgroup H such that $G=HP$ and $H \cap P = 1$. $(G = P \ltimes H)$.

Corollary: If G is simple and $p \mid |G|$, then $|G|=p$.

Pf of corollary:

$H \triangleleft G$ and $H \neq G$ (H is a p'-gp!). So $H=1$, and so G is a simple p-group, hence $|G|=p$.

Pf of Thm

Note that P is abelian, so we apply the previous theorem. Also, $C_P(N)=P$ because $P \leq Z(N_G(P))$. (Hence, by pt (iii) of thm, $[P,N]=1$).

By pt (ii), $P \cap \operatorname{Ker} \tau = [P,N] = 1$.

Let $H := \operatorname{Ker} \tau \triangleleft G$. $P \cap H = 1 \Rightarrow H$ is a p'-group.

Also, $G/H = G/\operatorname{Ker}\tau \simeq \operatorname{im} \tau = P^{\tau} = C_P(N) = P$

So $G = HP$, (by order considerations).

Application:

Let G be a finite non-abelian simple group, and let p be the smallest prime dividing $|G|$. Then $|G|$ is divisible by p^3 or 12.

Also, the Sylow-p-subgroups are not cyclic.

(Note: by Feyt-Thomson thm, $p=2$, and so it says $|G|$ divisible by 8 or 12).

Pf Let P be a Sylow p subgroup of G. Write $N = N_G(P)$, $C = C_G(P)$, so $C \trianglelefteq N$.
Suppose that P is cyclic of order p^m. Then $P \leqslant C \leqslant N$.
Then $|\operatorname{Aut} P| = (p-1)p^{m-1}$. Hence $|N/C| \mid |\operatorname{Aut} P|$ (because $N/C \simeq$ sgp of $\operatorname{Aut}(P)$).
So $|N/C| \mid p^{m-1}$ since p is the smallest prime. As N/C has order a p'-number, need $N=C$.

(cont pf)

$\therefore P \leq Z(N_G(P))$, which is impossible by Burnside. So P is not cyclic.

Assume now $p^3 \nmid |G|$. Will show that $12 \mid |G|$.

$p^3 \nmid |G| \Rightarrow |P| = p^2$, and so $P \simeq \mathbb{Z}/p \times \mathbb{Z}/p$ (as it is not cyclic).

So $\mathrm{Aut}(P) \simeq Gl_2(p)$, and $|\mathrm{Aut}(P)| = (p^2-1)(p^2-p) = p(p+1)(p-1)^2$.

Then $|N:C| \mid p(p-1)^2(p+1)$. Since $P \leq C$, $|N:C|$ is a p'-number.

$\therefore |N:C| \mid p+1$.

If p is odd, this would yield a prime $< p$ dividing $|G|$. Hence $p=2$, and $|N:C| = 3$.

Hence $4 \cdot 3 = 12 \mid |G|$.

//

Theorem (Hölder - Burnside - Zassenhaus):

i) Let G be a finite group, with all of its Sylow-subgroups cyclic. Then,

$$G = \langle x \rangle \ltimes \langle a \rangle$$

where if $|x| = m$, $|a| = n$, $(0<r<n)$ $a^x = a^r$ and n is odd, $r^m \equiv 1 \pmod n$, and $\gcd(n, m(r-1)) = 1$.

Also, $G' = \langle a \rangle$.

ii) Any such G has cyclic Sylow subgroups.

Pf/ Note that G cannot be simple, by the previous corollary. So $\exists\, \overset{\neq}{N} \overset{\neq}{\trianglelefteq} G$.

Note that N and G/N inherit the properties of G.

(if P is a sylow p-sgp of G, then PN/N is one of G/N).

By induction hypothesis, the result is true for N and G/N, so these groups are solvable, and G is solvable. Let $d = d(G)$, its derived length.

If $d \leq 1$, we are in the abelian case, so G is the direct product of its cyclic p-groups, for different p's. This is the case $n=1$.

↓

(cont pf). So can assume $d > 1$. Suppose $d > 2$:

Next note that $G^{(d+1)}$ is abelian, with cyclic Sylows $\Rightarrow$ $G^{(d+1)}$ is cyclic.

Hence, $\mathrm{Aut}(G^{(d-1)})$ is abelian, $\Rightarrow$ $G/C_G(G^{(d-1)})$ is abelian.

Hence, $G' \leq C_G(G^{(d-1)}) \Rightarrow [G^{(d-1)}, G'] = 1. \Rightarrow [G^{(d-1)}, G^{(d-2)}] = 1 \Rightarrow$

$\Rightarrow G^{(d-2)}$ is nilpotent of class ≤ 2 (since $G^{(d-2)}/G^{(d-1)}$ is abelian).

So $G^{(d-2)}$ is the direct product of its Sylows of cyclic groups $\Rightarrow G^{(d-2)}$

is abelian $\Rightarrow (G^{(d-2)})' = G^{(d-1)} = 1 \Rightarrow !!$ So $d = 2$.

Then, G' is abelian. $\therefore$ G' and G/G' are both cyclic.

Let Q be a Sylow-p-sgp of G. So Q is cyclic. By the second transfer thm for abelian sgps, $Q = C_Q(N) \times [Q, N]$, $N = N_G(Q)$.

As Q is a p-group and cyclic, one of the two factors is trivial:

Either $Q = [Q,N] \leq G'$ or $[Q,N] = 1$, and so $(Q \cap \ker(\overset{\text{the transfer}}{\tau})) = 1$

Hence, $Q \cap G' = 1$. (since $G' \leq \ker \tau$).

So either $Q \leq G'$ or $Q \cap G' = 1$. $\forall$ Sylow-p- of G.

Hence $\gcd\{|G'|, |G/G'|\} = 1$.

Put $m := |G/G'|$, $n := |G'|$, $\gcd(m,n) = 1$

Then $|G| = mn$, let $G' = \langle a \rangle$, $G/G' := \langle x_1 G' \rangle$. $|a| = n$, $|x_1| = m \cdot n_1$ for some $n_1 | n$. Define $x := x_1^{n_1}$ (so $|x| = m$), and $G/G' = \langle x G' \rangle$.

Therefore, $G = \langle x \rangle \ltimes \langle a \rangle$

Clearly, $a^x = a^r$ where $1 \overset{r=1 \Rightarrow \text{abelian}}{<} r < n$, and $(r,n) = 1$ (it is an isomorphism).

Since $x^m = 1$, $a^{x^m} = a^{r^m} = a$, so $r^m \equiv 1 \pmod{n}$. Note that $G' = \langle [a,x] \rangle$

As $[a,x] = a^{r-1}$, $G' = \langle a^{r-1} \rangle = \langle a \rangle$. So $\gcd(r-1, n) = 1$

Since $\gcd(n,r) = 1 = \gcd(n, r-1) \Rightarrow n$ is odd.

Pf of part (ii):

Let $G = \langle x\rangle \ltimes \langle a\rangle$, $m = |x|$, $n = |a|$, relatively prime.

Let P be a Sylow-p-sgp of G. ~~If~~

Then either $P \cap \langle a\rangle = 1$ or $P \subseteq \langle a\rangle$. (Since $(m,n) = 1$).

But if $P \subseteq \langle a\rangle$, P is cyclic. If $P \cap \langle a\rangle = 1$, then $P \cong P\langle a\rangle/\langle a\rangle \leq G/\langle a\rangle$ which is cyclic, also. //

Corollary: Any group of squarefree order satisfies the theorem.

Remark: Let $Sq(x)$ be the number of squarefree integers n, $1 \leq n \leq x$.

Then $Sq(x) = \frac{6}{\pi^2}x + O(\sqrt{x})$. So $\frac{Sq(x)}{x} \to \frac{6}{\pi^2} \simeq .6079$.

Example: Find all ~~all gro~~ groups of order $105 = 3\cdot5\cdot7$.

Then $G = \underset{m}{\langle x\rangle} \ltimes \underset{n}{\langle a\rangle}$, $mn = 105$, $a^x = a^r$.

$r^m \equiv 1 \pmod{n}$, $\gcd(n, (r-1)m) = 1$.

n	1	3	5	7	$3\cdot5$	$5\cdot7$	$3\cdot7$
m	$3\cdot5\cdot7$	$5\cdot7$	$3\cdot7$	$3\cdot5$	7	3	5
r	1	Imp	Imp	$2,4$	Imp	Imp	Imp

↑
abelian

Note that $|\mathrm{Aut}\langle a\rangle| = \varphi(n)$. If $\gcd(m, \varphi(n)) = 1$, then must have $r = 1$. This rules out the cases $n = 3, 5, 3\cdot5, 3\cdot7$

The case $n = 5\cdot7$, $m = 3$ is still possible. But $3 \nmid \varphi(5)$, so $r \equiv 1 \pmod 5$ so that $\mathrm{Aut}\langle a\rangle$ will act trivially on the 5-part.

But $\gcd(r-1, m) = 0 \Rightarrow$!!

$n = 7$, $m = 3\cdot5$ is possible, with two possibilities for r, 2 and 4, leading to isomorphic groups. So we get only two groups of order 105:

$\mathbb{Z}_{105}$, and $\underset{3\cdot5}{\langle x\rangle} \ltimes \underset{7}{\langle a\rangle}$, $a^x = a^2$ (note that $a^{x^{-1}} = a^4$, so $r = 2$ and 4 are isomorphic)

§6. Free Groups and Generators & Relations.

Def A free group F is, given a nonempty set X, a group with $\sigma : X \to F$ a set-map, and (F, σ) is free iff, given any function $\alpha : X \to G$, where G is any group, then $\exists!\ \beta : F \to G$ s.t.

$$\begin{tikzcd} & F \arrow[dr, dashed, "\exists!"] \arrow[d, phantom, "\Delta"] & \\ X \arrow[ur, "\sigma"] \arrow[rr, "\alpha"'] & & G \end{tikzcd}$$

commutes.

(F is a free object in the category of Gps).

One has to show that free groups exist. First, we prove a lemma:

Lemma: Let (F, σ) be free on X. Then:

(i) σ is injective

(ii) $\operatorname{im}(\sigma)$ generates F.

Pf (i) Assume $(x_1)\sigma = (x_2)\sigma$ [illegible] $(x_i \in X)$. Let G be a group with at least two elements, and let $g_1 \neq g_2$ in G.

$$\begin{tikzcd} & F \arrow[dr, dashed, "\exists!\beta"] & \\ X \arrow[ur, "\sigma"] \arrow[rr, "\alpha"] & & G \\ x_1 \arrow[rr, mapsto] & & g_1 \\ x_2 \arrow[rr, mapsto] & & g_2 \end{tikzcd}$$

~~So $\beta(\sigma(x_1)) = g_1 \neq g_2 = \beta(\sigma(x_2))$.~~

Then $(x_1)\sigma\beta = (x_2)\sigma\beta \Rightarrow x_1\alpha = x_2\alpha \Rightarrow g_1 = g_2 \Rightarrow !!$

(ii)

$$\begin{tikzcd} & F \arrow[d, dashed, "\exists!\beta"] \arrow[drr, dashed, bend left, "\beta i = id_F"] & & \\ X \arrow[ur, "\sigma"] \arrow[r, "\sigma'"'] & \langle \operatorname{im} \sigma \rangle \arrow[rr, hook, "i"] & & F \end{tikzcd}$$

where $(x)\sigma' = (x)\sigma$

Hence, $\exists!\ \beta : F \to \langle \operatorname{im} \sigma \rangle$ s.t. $\sigma\beta = \sigma'$.

So $\beta i : F \to F$, and $\sigma\beta i = \sigma' i = \sigma = \sigma\, id_F$

By uniqueness, $\beta i = id_F \Rightarrow i$ is surjective, so it is a bijection, hence $\langle \operatorname{im} \sigma \rangle = F$. //

Conclusion: we don't loose anything if we assume $X \subseteq F$.

Theorem: Let X be any non-empty set. Then there is a group F and a function $\sigma : X \to F$ s.t. (F, σ) is free on X.

Pf The idea is to form the "largest" group that can be "generated" by X.
Choose a set disjoint from X with the same cardinal, and call it $X^{-1} := \{x^{-1} : x \in X\}$. (formal symbols). $\left(X \overset{1:1}{\Longleftrightarrow} X' , \quad X \cap X^{-1} = \emptyset \right)$.

By a word in X, we understand a finite sequence of elements coming from $X \cup X^{-1}$, written as $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}$, where $x_i \in X$, $\varepsilon_i = \pm 1$.
(for $k \geq 0$, as $k=0$ gives us the empty word, denoted by 1).

Write S for the set of all words on X.

Define a product in S by juxtaposition (if one of the words is the empty word, we get the same word): $w1 = 1w = w$.
This is clearly an associative operation.

Define the "inverse" of $w = x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$, as $w^{-1} = x_k^{-\varepsilon_k} \dots x_1^{-\varepsilon_1}$.

Note that so far S is a monoid. We still need to be able to cancel $x x^{-1}$.

For it, we introduce a relation on S, called $\sim$, as:

$v \sim w \Leftrightarrow$ it is possible to pass from v to w by a finite sequence of operations of two types:

- → insertion of the subsequence $x^{-1}x$ or xx^{-1} $(x \in X)$.
- → deletion of — — — " — —

Clearly this is an equivalence relation. Write $[w]$ for the equivalence class of w.

Let $F = S/_{\sim} = \{[w] \mid w \in S\}$, and define $[w] \cdot [v] := [w \cdot v]$.
It will be a well defined product: $w \sim w'$, $v \sim v' \Rightarrow wv \sim w'v'$ (ok).
Also, $[w][1] = [1][w] = [w]$, and $[w][w^{-1}] = [ww^{-1}] = [1]$.

d

(cont pf).

Now, define $\sigma: X \to F$ by $(x)\sigma := [x]$. Notice that $F = \langle \mathrm{im}\, \sigma \rangle$, because ~~W~~ $w \in S$ and $w = x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$, then $[w] = [x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}] = [x_1]^{\varepsilon_1} \dots [x_k]^{\varepsilon_k} =$

$= ((x_1)\sigma)^{\varepsilon_1} \dots ((x_k)\sigma)^{\varepsilon_k}$. ✓.

Claim: (F, σ) is free on X.

Let $\alpha: X \to G$ be any given map, with G a group.

Need to define

$$\begin{tikzcd} & F \arrow[d, dashed, "\beta"] \\ X \arrow[ur, "\sigma"] \arrow[r, "\alpha"'] & G \end{tikzcd}$$

First, define $\beta': S \to G$ by the rule $(x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k})^{\beta'} := (x_1^{\alpha})^{\varepsilon_1} \dots (x_k^{\alpha})^{\varepsilon_k} \in G$.

This induces a unique map on F, as $w \sim v \Rightarrow w^{\beta'} = v^{\beta'}$. Call it $\beta: F \to G$.

↑ in G, these cancel.

(Define $[w]^{\beta} := w^{\beta'}$, $w \in S$)

We want β to be a homomorphism:

$$([v][w])^{\beta} = [vw]^{\beta} = (vw)^{\beta'} = v^{\beta'} w^{\beta'} = [v]^{\beta} [w]^{\beta} \quad ✓.$$

Also, $\sigma\beta = \alpha$, because $x^{\sigma\beta} = [x]^{\beta} = x\beta' = x^{\alpha}$ ✓.

Finally, ~~uniqueness~~ let $\gamma: F \to G$ be another gp homomorphism, s.t. $\sigma\gamma = \alpha$.

Then $\sigma\gamma = \sigma\beta$. But note that $\langle \mathrm{im}\, \sigma \rangle = F$, since if $f \in F$, $f = [x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}] = [x_1]^{\varepsilon_1} \dots [x_k]^{\varepsilon_k} = (x_1^{\varepsilon_1})^{\sigma} \dots (x_k^{\varepsilon_k})^{\sigma} \in \langle \mathrm{im}\, \sigma \rangle$

Hence, $\gamma = \beta$. $\Rightarrow$ (F, σ) is free on X.

We introduce next the concept of reduced words.

Def A word in S is <u>reduced</u> if it does not contain a subsequence xx^{-1} or $x^{-1}x$.

Lemma: Every equivalence class of words contains a reduced word.

Pf Consider $[w]$: if w is reduced, done. Otherwise, it contains xx^{-1} or $x^{-1}x$. Can delete it, ~~thus~~ getting a shorter word in the same class. Apply induction. //

Theorem: Every equivalence class contains a <u>unique</u> reduced word.

Pf A direct approach is difficult. Instead, we use a permutation representation (due to B.H. Neumann).

Let F be free on X, as constructed.

Let R be the set of all reduced words in X.

Define a permutation rep'n of F on R: if $u \in X \cup X^{-1}$, define $u' \in Sym(R)$ by

Let $x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \in R$. Then $(x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k})u' := \begin{cases} x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} u & \text{if } u \neq x_k^{-\varepsilon_k} \\ x_1^{\varepsilon_1} \cdots x_{k-1}^{\varepsilon_{k-1}} & \text{if } u = x_k^{\varepsilon_k} \end{cases}$

(and note that the new word is reduced!).

It is in fact a permutation as $(u')^{-1} = (u^{-1})'$. Hence $u' \in Sym(R)$.

$$\begin{tikzcd} & F \arrow[d, dashed, "\beta"] \\ X \arrow[ru, "\sigma"] \arrow[r, "\alpha"'] & Sym(R) \end{tikzcd}$$

G

where $\alpha: x \mapsto x'$

Will apply the mapping property, to get a homomorphism $\beta: F \to Sym(R)$

So $\sigma\beta = \alpha$. Hence $x^{\alpha} = x^{\sigma\beta} = [x]^{\beta} \quad \forall x \in X$.

Now, suppose that $[v] = [w]$, where v, w are reduced. We'll show $v = w$:

Write $v = x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}$ (reduced form). Then, $[v]^{\beta} = [w]^{\beta}$, and

$$[v]^{\beta} = \left([x_1^{\varepsilon_1}] \cdots [x_k^{\varepsilon_k}]\right)^{\beta} = \left((x_1^{\sigma})^{\varepsilon_1}\right)^{\beta} \cdots \left((x_k^{\sigma})^{\varepsilon_k}\right)^{\beta} = (x_1^{\sigma\beta})^{\varepsilon_1} \cdots (x_k^{\sigma\beta})^{\varepsilon_k} =$$
$$= (x_1^{\alpha})^{\varepsilon_1} \cdots (x_k^{\alpha})^{\varepsilon_k} = (x_1')^{\varepsilon_1} \cdots (x_k')^{\varepsilon_k}$$

Apply $[v]^{\beta}$ to the empty word 1, to get $x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} = v$

So $[v]^{\beta} = [w]^{\beta} \Rightarrow v = w$ //

Normal Form in Free Groups.

Each $f \in F$ has a unique form $f = [w]$, where w is a reduced word, $w = x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}$. Then $f = [x_1]^{\varepsilon_1} \cdots [x_k]^{\varepsilon_k}$.

Combine $[x_i]^{\varepsilon_i}$'s that are consecutive, and so one can write:

$$f = [x_{i_1}]^{l_1} [x_{i_2}]^{l_2} \cdots [x_{i_r}]^{l_r} \quad \text{, where } 0 \neq l_i \in \mathbb{Z} \text{ and } x_{i_j} \neq x_{i_{j+1}},\ r \geq 0.$$

This expression for f is unique.

For convenience, we identify x with its equivalence class, $[x]$, and so $X \subseteq F$. Then, X is a "special" set of generators for F, called a <u>normal form</u>.

If $f \in F$, then $f = x_{i_1}^{l_1} \cdots x_{i_r}^{l_r}$ uniquely with $\overset{0}{\neq} l_i \in \mathbb{Z}$, $x_{i_j} \neq x_{i_{j+1}}$, $r \geq 0$.

Conversely,

<u>Theorem:</u> Let G be a group with a set of generators X, such that each $g \in G$ has a unique expression $g = x_{i_1}^{l_1} \cdots x_{i_r}^{l_r}$, $x_i \in X$. $x_{i_j} \neq x_{i_{j+1}}$, $0 \neq l_i \in \mathbb{Z}$, $r \geq 0$.

Then, G is free on X.

Pf Let F be free group on X, constructed as before.

$$\begin{tikzcd} & F \\ X \arrow[ur, "\sigma"] \arrow[r, hook, "i"] & G \end{tikzcd}$$

By the mapping property, $\exists!\ \beta : F \longrightarrow G$ s.t. $\sigma\beta = i$.

We want to prove that β is an isomorphism.

First, β is surjective, since $G = \langle X \rangle$, and $\sigma\beta = i$ ✓.

Suppose $[x_{i_1}]^{l_1} \cdots [x_{i_r}]^{l_r} \in \ker\beta$. As $[x]^{\sigma}\beta = x$, then

$$x_{i_1}^{l_1} \cdots x_{i_r}^{l_r} = 1_G \xRightarrow{\text{uniqueness of the expression for } 1_G} r = 0 \Rightarrow \checkmark.$$

So $\beta : F \xrightarrow{\cong} G$ is iso.

• Uniqueness of free groups

Let (F_1, σ_1), (F_2, σ_2) be free on X_1, X_2, respectively, where $|X_1| = |X_2|$.

Then $F_1 \simeq F_2$:

Pf Let $\alpha : X_1 \to X_2$ be a bijection.

$$\begin{tikzcd}
& F_1 \arrow[dr, dashed, "\beta_1"] \arrow[d, phantom, "G"] & \\
X_1 \arrow[ur, "\sigma_1"] \arrow[rr, "\alpha\sigma_2"'] & {} & F_2
\end{tikzcd}
\qquad
\begin{tikzcd}
& F_2 \arrow[dr, dashed, "\beta_2"] \arrow[d, phantom, "G"] & \\
X_2 \arrow[ur, "\sigma_2"] \arrow[rr, "\alpha^{-1}\sigma_1"'] & {} & F_1
\end{tikzcd}
\quad \text{i.e.} \left\{ \begin{aligned} \sigma_1 \beta_1 &= \alpha \sigma_2 \\ \sigma_2 \beta_2 &= \alpha^{-1} \sigma_1 \end{aligned} \right.$$

Hence, $\sigma_1(\beta_1\beta_2) = \alpha\sigma_2\beta_2 = \alpha\alpha^{-1}\sigma_1 = \sigma_1$. So the following diagram commutes:

$$\begin{tikzcd}
& F_1 \arrow[dr, "\beta_1\beta_2"] \arrow[dr, bend left, "id"] \arrow[d, phantom, "G"] & \\
X_1 \arrow[ur, "\sigma_1"] \arrow[rr, "\sigma_1"'] & {} & F_1
\end{tikzcd}
\Rightarrow \beta_1\beta_2 = id_{F_1}, \text{ and } \beta_2\beta_1 = id_{F_2}. \quad ✓$$

• Examples of free groups.

1. Let α, β be functions on $\mathbb{C} \cup \{\infty\}$ defined by $\alpha : z \mapsto z+2$

where ∞ is subject to natural rules $\left\{ \begin{aligned} &\infty + 2 = \infty \\ &\frac{\infty}{1+2\infty} = \frac{1}{2} \end{aligned} \right.$, ... $\quad \beta : z \mapsto \dfrac{z}{1+2z}$

Then α, β are bijective (so they are permutations of $\mathbb{C} \cup \infty$).

Let $F = \langle \alpha, \beta \rangle$. Then,

Theorem: F is freely generated by α and β.

Pf want to show that there is a normal form in the generators.

i.e. there is no nontrivial word $W = \alpha^{m_1}\beta^{n_1}\alpha^{m_2}\beta^{n_2}\ldots$ $(m_i, n_i \in \mathbb{Z})$.

such that $W = 1$ in F.

Will use a geometric argument. Observe:

i) A nontrivial power of α maps the interior unit circle to the exterior, not including ∞.

ii) A nontrivial power of β maps the exterior of the unit circle (including ∞) to the interior, but with 0 removed. (Just observe $\beta(\frac{1}{z}) = \frac{1}{z+2}$).

Now, if $m_1 \geq 0$, then W cannot fix 0. Hence $W \neq 1$. ✓

Example 2: Linear fractional transformations

Define a map on $\mathbb{C}\cup\infty$ as $\lambda(a,b,c,d): z \longmapsto \frac{az+b}{cz+d}$ (bijective if $ad-bc\neq 0$).
Call this a linear fractional transformation.

These form a group $L(\mathbb{C})$ (linear fractional group on $\mathbb{C}$).

Define a map

note that it is transposed !!

$$\Theta: Gl_2(\mathbb{C}) \longrightarrow L(\mathbb{C}) \qquad \text{is a surjective homomorphism.}$$

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \longmapsto \lambda(a,b,c,d)$$

Ker Θ is the subgroup of 2×2 scalar matrices $c\mathbb{1}_2$, $0\neq c\in\mathbb{C}$.

So $L(\mathbb{C}) \simeq Gl_2(\mathbb{C})/\mathbb{C}^* = PGL_2(\mathbb{C})$

Recall that $\alpha,\beta\in L(\mathbb{C})$ (from previous example) $\begin{cases}\alpha(z)=z+2\\ \beta(z)=\frac{z}{2z+1}\end{cases}$

Put $A=\begin{pmatrix}1&0\\2&1\end{pmatrix}$, $B=\begin{pmatrix}1&2\\0&1\end{pmatrix}$.

Put $G := \langle A,B\rangle \leq SL_2(\mathbb{Z}) \leq GL_2(\mathbb{Z})$.

Then $\Theta|_G : G \twoheadrightarrow F$. This means that G is free on A, B, because:

if $A^{m_1}B^{n_1}\cdots A^{m_k}B^{n_k}=1$ in G, then $\alpha^{m_1}\beta^{n_1}\cdots\alpha^{m_k}\beta^{n_k}=1$ in F

$\Rightarrow m_i, n_i = 0$.

Hence, there's a normal form for G in A, B. ($\Rightarrow$ G free).

Theorem (J.Tits): if G is a f.gen subgroup of $Gl_n(F)$, where F is a field,
(1970's) then either G contains a free subgroup of rank 2,
or else G is an extension of a soluble group by
a finite group.

- Fundamental property of free groups.

Suppose $G = \langle X \rangle$, let F be free on a subset $Y \subseteq X$. If $\alpha : Y \to X$ is surjective, then α extends to an homomorphism $\theta : F \longrightarrow G$, so $G \simeq F/\ker\theta$.

Pf/ θ exists by the mapping property //

- Elementary properties of free groups.

1. Free groups are torsion-free.

Let F be free on $X \subseteq F$, and let $1 \neq f \in F$. Then

$f = x_{i_1}^{l_1} \cdots x_{i_r}^{l_r}$, $x_{i_j} \in X, X_{i_j} \neq X_{i_{j+1}}$ (normal form).

Suppose $f^m = 1$, $m > 0$.

We can assume $i_1 \neq i_r$, for else we could replace f by $f^{(x_{i_1}^{l_1})^{-1}} = x_{i_2}^{l_2} \cdots x_{i_{r-1}}^{l_{r-1}} x_{i_r}^{l_r + l_1}$, (if $i_1 = i_r$), (this is called cyclic reduction).

So assume $i_r \neq i_1$. Then,

$f^m = x_{i_1}^{l_1} \cdots x_{i_r}^{l_r} x_{i_1}^{l_1} \cdots x_{i_r}^{l_r} \cdots \neq 1$ $\rightarrow$!!

//

· Presentations.

Let G be a group, then there is a surjective hom $\pi : F \to G$, where F is the free group. Then $G \simeq F/R$, where $R = \ker \pi \trianglelefteq F$, and there is an exact sequence: $1 \to R \to F \to G \to 1$.

The elements of R are called <u>relators</u>. We say that $r = 1$ is a <u>relation in G</u>.

Choose any set of generators X for G. Let Y be any set with $|X| = |Y|$, and let F be free on Y, say $\sigma : Y \to X$ is some bijection, then it determines a homomorphism $F \longrightarrow G$ with kernel R. Choose $S \subseteq R$ such that $R = S^F = \langle s^f : s \in S, f \in F \rangle$ (normal closure of S in F).

Then each relator can be written as $r \in R$,

$$r = (s_1^{\varepsilon_1})^{f_1} \cdots (s_k^{\varepsilon_k})^{f_k} \quad \text{where } \begin{cases} \varepsilon_i = \pm 1 \\ f_i \in F \end{cases}.$$

Then we say that r is a <u>consequence of S</u>.

<u>Def</u>: A <u>presentation</u> of G is $G = \langle \overset{\text{generators}}{X} \mid \overset{\text{defining relators}}{S} \rangle$.

Conversely, if we start with a set X and $\overset{\text{subset of } F_X}{S} \subseteq F_X$ (free group on X). Then one can form a presentation $\langle X \mid S \rangle$ by defining $G := F_X / S^{F_X}$. This group has a presentation $\langle X \mid S \rangle$, obviously.

<u>**Von Dyck's Thm**</u>: Let G, H be groups with presentations $\langle X \mid S \rangle$, $\langle Y, T \rangle$.
Suppose that $\sigma : X \to Y$ is a bijection s.t. S^σ is a consequence of T.
Then there is a surjective homomorphism $\theta : G \twoheadrightarrow H$.

Pf Let F_X, F_Y be free on X and Y. Then $G = F_X / S^{F_X}$, $H = F_Y / T^{F_Y}$.
We have $\sigma : X \to Y$, can extend it to $\sigma : F_X \to F_Y$. Note that
$(S^{F_X})^\sigma = (S^\sigma)^{F_Y} \subseteq (T^{F_Y})^{F_Y} = T^{F_Y}$. Hence can define $\theta : F_X / S^{F_X} \to F_Y / S^{F_Y}$
by $(f S^{F_X})^\theta = f^\sigma T^{F_Y}$ which is well-defined & surj.

//

Examples of presentations.

1. $\langle x \mid \emptyset \rangle = \langle x \rangle$, infinite cyclic gp.

2. $\langle x \mid x^n \rangle = \langle x \rangle / \langle x^n \rangle \cong \mathbb{Z}/n\mathbb{Z}$, cyclic group of order n. $(n > 0)$.

3. $\langle x, y \mid x^2, y^2 \rangle =: G$.

Consider the infinite dihedral group $D = \langle u \rangle \ltimes \langle v \rangle$ $\begin{cases} \langle v \rangle \ \infty\text{-cyclic} \\ |\langle u \rangle| = 2 \\ v^u = v^{-1} \end{cases}$

Put $w = uv$. Then $w^2 = uvuv = (u^{-1}vu)\,v = v^{-1}v = 1$

Clearly, $D = \langle u, w \rangle$. By Von Dyck's Thm, there is a surjective hom.

$\theta : G \to D$, mapping $\begin{matrix} x \mapsto u \\ y \mapsto w \end{matrix}$ $\therefore$ $G/\ker\theta \cong D$.

We want to see that $\ker \theta = 1$.

Suppose that $g \in \ker(\theta)$. We can assume either $g = \begin{cases} (xy)^r \\ (xy)^r x \end{cases}$

(because if g starts with y, then replace it by $y^{-1}gy \in \ker(\theta)$)

Now $(xy)^\theta = x^\theta y^\theta = uw = u^2v = v \Rightarrow$ either $\begin{cases} v^r = 1 \Rightarrow r = 0 \\ v^r u = 1 \Rightarrow !! \end{cases}$ $\Rightarrow \ker\theta = \{1\}$.

Hence $G \cong D$.

4. $G = \langle x, y \mid x^4, y^2, (xy)^3 \rangle$.

Put $X = \langle x \rangle$. Then $|X| \leq 4$.

Then, use the method of "coset enumeration" (to try to prove it's finite).

Define $\mathcal{S} = \{ X, Xy, Xyx, Xyx^2, Xyx^3, Xyx^2y \}$.

Claim: $\mathcal{S}$ is the set of all cosets of X in G.

Observe that it's enough to prove that $\mathcal{S}x = \mathcal{S}$, and $\mathcal{S}y = \mathcal{S}$.

Note that $x^{-1} = x^3$, $y^{-1} = y$, $x(yxy)xy = 1 \Rightarrow yxy = x^3yx^3$.

Also, $xyx = yx^3y$.

To show $\mathcal{S}x = \mathcal{S}$, only need that $Xyx^2yx \in \mathcal{S}$. But $Xyx^2yx = X(yx)(xyx) = X(yx)(yx^3y) = X(x^3yx^3x^3y) = Xyx^2y \in \mathcal{S}$. The $\mathcal{S}y = \mathcal{S}$ is easy.

(cont example).

This gives a bound for $|G|$: $|X| \leq 4$, $|G/H| \leq 6 \Rightarrow |G| \leq 24$.

As it have to have elements of order 2, 3, 4, might try S_4.

Put $\bar{x} = (1234)$, $\bar{y} = (12)$. $(\bar{x}^4 = 1,\ \bar{y}^2 = 1,$ and $(\bar{x}\bar{y})^3 = 1)$.

Applying von Dycke, we get a surjective hom $G \twoheadrightarrow S_4 \Rightarrow G \cong S_4$.

<u>Example 5</u>: $G = \langle x, y \mid x^3, y^3, (xy)^3 \rangle$. $\Big|$ note that $xyx = y^2x^2y^2$

$yxy = x^2y^2x^2$

Put $a := x^2y$, $b = xyx$

Write $H := \langle a, b \rangle \leq G$.

<u>Claim</u>: $H \trianglelefteq G$.

$x^{-1}ax = xyx = b \in H$. ; $x^{-1}bx = x^{-1}(xyx)x = yx^2 = (a^{-1}b^{-1} = yx^2)$

~~$y^{-1}ay = yx^2y^2 = y^{-2}yx^2y^2$~~

Note that $G = \langle x, H \rangle$, and so $H^x \leq H \Rightarrow H = H^{x^3} \leq H^{x^2} \leq H^x \leq H$

$\Rightarrow H = H^x$. Since $G = \langle x, H \rangle$, then $H \trianglelefteq G$. $\lrcorner$

Next, note that:

$ab = x^2yxyx = x^2(yxy)x = x^2 \cdot (x^2y^2x^2)x = xy^2$
$ba = xyxx^2y = xy^2$
$\Big\} \Rightarrow ab = ba \Rightarrow$

$\Rightarrow H = \langle a, b \rangle$ is abelian.

So $G = \langle x \rangle \cdot H$ $(H \trianglelefteq G)$ and H is abelian. Also, $a^x = b$, $b^x = a^{-1}b^{-1}$.

We construct now a group with these properties.

Let $\bar{H} := \langle \bar{a}, \bar{b} \rangle$, free abelian of rank 2.

Let $|\langle \bar{x} \rangle| = 3$, and let $\bar{x}$ act on $\bar{H}$ by $\bar{a}^{\bar{x}} = \bar{b}$, $\bar{b}^{\bar{x}} = \bar{a}^{-1}\bar{b}^{-1}$

($\bar{x}$ is acting as $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, which has indeed order 3).

Form the semidirect product $\bar{G} = \langle \bar{x} \rangle \ltimes \bar{H}$ with the previous action.

Define $\bar{y} := \bar{x}^{-2}\bar{a}\cancel{\bar{x}}\bar{a}$ (taken from the relation $a = x^2y$).

$\downarrow$

(cont example).

Note that $\bar{G} = \langle \bar{x}, \bar{y} \rangle$ since $\bar{a}, \bar{b} \in \langle \bar{x}, \bar{y} \rangle$.

Note next that $\bar{x}^3 = 1$, $\bar{y}^3 = (\bar{x}\bar{a})^3 = \bar{x}\bar{a}\bar{x}\bar{a}\bar{x}\bar{a} = \bar{x}^2\bar{b}\bar{a}\bar{x}\bar{a} = \underbrace{\cancel{\bar{x}}^3(\bar{a}^{-1}\bar{b}^{-1})\bar{b}\bar{a}}_{= 1}$.

Also, $(\bar{x}\bar{y})^3 = 1$ (Check as exercise).

So the defining relations hold in G. By von Dyck, get a surjective hom.

$\theta : G \twoheadrightarrow \bar{G}$.

A typical element of G has the form $x^i a^j b^k$, which maps to $\bar{x}^i\bar{a}^j\bar{b}^k$. If $\bar{x}^i\bar{a}^j\bar{b}^k = 1$ in $\bar{G} = \langle \bar{x} \rangle \ltimes \bar{M}$, then $\bar{x}^i = 1$ and $\bar{a}^j\bar{b}^k = 1$. $\Rightarrow i \equiv 0\ (3)$, and $j = k = 0$. So $x^i a^j b^k = 1 \Rightarrow$

$\Rightarrow \theta$ is an isomorphism. //

Groups like $\langle x, y \mid x^m, y^n, (xy)^l \rangle$ are called triangle groups, and they are hard to study. Note however that the case $m = n = l$ is easier, and we got that G was actually polycyclic.

Finitely presented groups.

Def: A group G is finitely presented if it has a finite presentation, i.e.

$G = \langle x_1, \dots, x_m \mid r_1, \dots, r_k \rangle$ (both m, k finite).

Example: $\mathbb{Z} \text{ wr } \mathbb{Z}$ is finitely generated (and soluble). But it is not finitely presented (it is not obvious).

The property of being finitely-presented is independent of the presentation:

Theorem: Let G be a finitely-presented group, and assume G is generated by X, for some $X \subseteq G$. Then G has a presentation $G = \langle X_0 \mid S \rangle$ where $X_0 \subseteq X$ is finite, and S is finite.

(due to (BH Neumann))

Pf of Theorem (BH Neumann).

Let $G = \langle y_1, \ldots, y_m \mid s_1, \ldots, s_\ell \rangle$ be the given finite presentation.

Since $G = \langle X \rangle$, we have $G = \langle x_1, \ldots, x_n \rangle$ finite, where $x_i \in X$

(because each of the y_j is expressible in terms of elements of X.

Hence $y_i = w_i(\underline{x})$ ($w_i(\underline{x})$ is a word in $x_1, \ldots, x_n$).

Also, $x_j = v_j(\underline{y})$. Then the following relations in the x_j's hold:

$$\begin{cases} s_k\left(w_1(\underline{x}), \ldots, w_m(\underline{x})\right) = 1 & k = 1, \ldots, \ell \\ \text{Also, } x_j = v_j\left(w_1(\underline{x}), \ldots, w_m(\underline{x})\right) & j = 1, 2, \ldots, n \end{cases}$$

So let $\bar{G} = \langle \underline{\bar{x}} \mid \bar{S} \rangle$ where $\bar{S}$ is the set of relations (finite!).

(i.e. $s_k\left(w_1(\bar{x}), \ldots, w_m(\bar{x})\right) = 1$, $v_j\left(w_1(\bar{x}), \ldots, w_m(\bar{x})\right) = 1$).

So $\bar{G}$ is finitely presented. We prove that $\bar{G} \cong G$.

By von Dyck's theorem, there is a surjective homomorphism $\theta : \bar{G} \twoheadrightarrow G$,

with $\bar{x}_j^{\theta} = x_j$.

Define $\bar{y}_i = w_i(\bar{x}) \in \bar{G}$, and note that $\bar{G} = \langle \bar{y}_1, \ldots, \bar{y}_m \rangle$

(because $\bar{x}_i = v_j(\underline{\bar{y}}) \in \langle \bar{y}_1, \ldots, \bar{y}_m \rangle$)

Next, $s_k(\underline{\bar{y}}) = s_k\left(w_1(\bar{x}), \ldots, w_m(\bar{x})\right) = 1$. { Hence all the defining relations of G hold in $\bar{G}$.

By von Dyck's thm again, $\exists\, \varphi : G \twoheadrightarrow \bar{G}$ with $y_i^{\varphi} = \bar{y}_i$.

$$\text{Then, } \begin{cases} \bar{x}_i^{\theta\varphi} = x_i^{\varphi} = v_i(\underline{y})^{\varphi} = v_i(\underline{\bar{y}}) = \bar{x}_i \\ y_i^{\varphi\theta} = \bar{y}_i^{\theta} = w_i(\underline{\bar{x}})^{\theta} = w_i(\underline{x}) = y_i \end{cases} \Rightarrow \varphi = \theta^{-1} \Rightarrow G \cong \bar{G}$$

Examples:

1) All cyclic groups are finitely presented.

2) All finite groups are finitely presented (as generators, all elements of G and for relations, the group table.)

Theorem (P. Hall): Let $N \trianglelefteq G$ and assume N, G/N are both finitely presented. Then G is finitely presented.

Corollary: All polycyclic groups are finitely presented.

Pf of Thm:

Assume we have $N = \langle x_1, \dots, x_m \mid r_1, \dots, r_k \rangle$, $G/N = \langle y_1 N, \dots, y_n N \mid s_1, \dots, s_\ell \rangle$

Then $G = \langle x_1, \dots, x_m, y_1, \dots, y_n \rangle$.

The next step is to write all the relations in these.

$$\left.\begin{array}{ll} r_i(\underline{x}) = 1 \,, & s_j(\underline{y}) = t_j(\underline{x}) \end{array}\right) \begin{array}{l} i = 1 \dots k \\ j = 1 \dots \ell \end{array}$$

$$\left.\begin{array}{ll} x_i^{y_j} = u_{ij}(\underline{x}) \,, & x_i^{y_j^{-1}} = u'_{ij}(\underline{x}) \end{array}\right) \begin{array}{l} i = 1 \dots m \\ j = 1 \dots n \end{array}$$

Next step, let $\bar{G}$ be the group with a presentation on generators $\bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n$, and defining relations in $\bar{x}_i$, $\bar{y}_i$. So $\bar{G}$ is a finitely presented group.

By von Dyck's, $\exists\ \theta : \bar{G} \twoheadrightarrow G$, with $\bar{x}_i^{\theta} = x_i$, $\bar{y}_j^{\theta} = y_j$.

Put $\bar{N} = \langle \bar{x}_1, \dots, \bar{x}_m \rangle$. Then $\bar{N} \trianglelefteq \bar{G}$, by the relations.

Next, note $\theta|_{\bar{N}} : \bar{N} \to N$ is an iso. (Von Dyck's implies $\varphi : N \twoheadrightarrow \bar{N}$ with $x_i^{\varphi} = \bar{x}_i$ and $\theta|_{\bar{N}}$ and φ are mutually inverse)

So $(\operatorname{Ker} \theta) \cap \bar{N} = 1$

Since $\bar{N}^{\theta} = N$, there is an induced homomorphism $\theta' : \bar{G}/\bar{N} \to G/N$, where $(\bar{y}_j \bar{N})^{\theta'} = \bar{y}_j^{\theta} N = y_j N$.

By von Dyck's, $\exists\ \psi : G/N \twoheadrightarrow \bar{G}/\bar{N}$, where $(y_j N)^{\psi} = \bar{y}_j \bar{N}$. Also, θ' and ψ are mutually inverses, so θ' is an iso. $\Rightarrow \operatorname{Ker} \theta \leq \bar{N} \Rightarrow \operatorname{Ker} \theta = 1$ //

Corollary (repeat): Every polycyclic group is finitely presented.

The Word Problem

Suppose that G is a group with a given finite presentation, $G = \langle X \mid R \rangle$.
Then the word problem asks if there is an algorithm which, when a word w in X is given, decides whether $w = 1$ in G.

Write S for the set of all words in X. (i.e. $w \in S$, $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}$ $\left(\begin{matrix} \varepsilon_i = \pm 1 \\ x_i \in X \end{matrix}\right)$)

One can enumerate all such words (i.e. S is recursively enumerable).
(this means that S is the output of some Turing machine).

Each relator of G is a consequence of the defining relators.

Recall that $F_X \twoheadrightarrow G$ with $\mathrm{Ker} = R^{F_X}$.

So anything in R^{F_X} will be $(r_1^{\pm 1})^{f_1} (r_2^{\pm 1})^{f_2} \cdots (r_k^{\pm 1})^{f_k}$ $\begin{matrix} r_i \in R \\ f_i \in S \end{matrix}$

Thus (needs a proof) $T = R^{F_X}$ is recursively enumerable.

So, if the given word w is a relator, it will eventually appear in the output of the Turing Machine.

What if $w \neq 1$?

$S \setminus T$ is the set of non-relators, and it might not be recursively enumerable
($\exists$ recursively enumerable sets which are not recursive (i.e. whose complement is not)).

If this is the case, the word problem cannot be solved.

In 1954, Boone & Novikov gave examples of finitely presented groups with unsolvable word problem.

However, the WP is solvable for many classes of finitely presented group.

Theorem: Let G be a finitely presented residually-finite group.
Then G has solvable word problem.

Pf/ Let $G = \langle x_1, \dots, x_n \mid s_1, \dots, s_k \rangle$, and let F be the free group on $\{x_1, \dots, x_n\}$.

Suppose w be a given word in $x_1, \dots, x_n$.

To decide whether $w = 1$ in G, we set two procedures in motion:

Ⓘ Enumerate all consequences of $s_1, \dots, s_k$ and look for w in the list.
If w appears, then $w = 1$ in G. $\Rightarrow$ STOP.

Ⓘⓘ Enumerate the finite groups, say by exhibiting their multiplication tables,
$G_1, G_2, \dots$

For each i, ~~G_i~~, construct all homomorphisms $\theta_{ij} : F \longrightarrow G_i$
(it's a finite list because F is fin.gen & G_i is finite).

Check if $s_i^{\theta_{ij}} = 1$ in G_i (so that θ_{ij} induces a hom. $G \to G_i$).

So we obtain all homomorphisms $G \to G_i$ $\quad i = 1, 2, \dots$

For each such θ_{ij}, check to see if $w^{\theta_{ij}} = 1$ in G_i.
If $w^{\theta_{ij}} \neq 1$ in G_i for some i, then $w \neq 1$ in G $\Rightarrow$ STOP.

Claim: One of these two procedures will stop.

$\rightarrow$ if $w = 1$ in G, Ⓘ will stop.

$\rightarrow$ if $w \neq 1$, $\exists\, N \triangleleft G$, $|G : N| < \infty$, and $w \notin N$.
So G/N will appear as G_i for some i, and $\theta_{ij}(w) \neq 1$ in G_i
$\Rightarrow$ Ⓘⓘ stops.

Reference: J. Rotman, "Group Theory".

Corollary: The word problem is solvable for a polycyclic group.

Pf/ We saw that polycyclic $\Rightarrow$ residually-finite.

Some other algorithmic problems.

1) The generalized word problem. (for G fin. presented).

Given words $W, W_1, \ldots, W_n$. Decide whether $W \in \langle W_1, \ldots, W_n \rangle$ in G.

2) The conjugacy problem. (G fin pres).

Given two words u, v. Decide if they are conjugate in G.

These are more difficult than the word problem (so they are unsolvable). But they are solvable for polycyclic groups.

3) The identity problem.

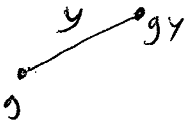
Decide if a finitely presented group G has order 1. ← not decidable! (Rabin, 1960).

But, given a fin. pres G, decide if $G = G'$. ← decidable.

The Cayley Graph.

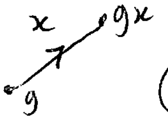
Suppose G is a group with a presentation $\langle X \mid R \rangle$.

Def The Cayley graph $C(X, R)$ is the graph with vertex set G, and with edges (g, gy) where $g \in G$, $y \in X \cup X^{-1}$, labeled with y:

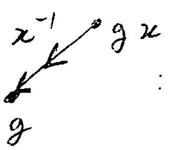


Note: the Cayley graph is connected.

One can think of the graph as directed, as

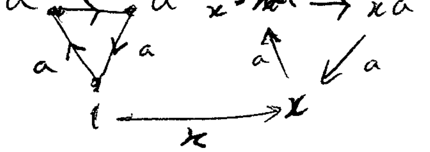


$(x \in X)$ or

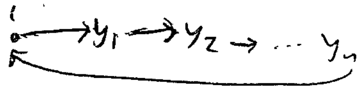


:

Example: $G = S_3$, $G = \langle x, a \mid x^2 = 1 = a^3, a^x = a^{-1} \rangle$.



In general, if $r = y_1 y_2 \cdots y_n$ is a relator, with $y_i \in X \cup X^{-1}$, then there is a corresponding cycle



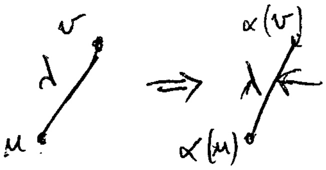
Conversely, each cycle leads to a relator.

If the group is free on X, there are no relators and so the graph is a <u>tree</u>.

Conversely, if the Cayley graph is a tree, the group is free.

<u>Automorphisms</u>

<u>Def</u>: An <u>automorphism α of a labeled graph</u> is a permutation of the vertex set which preserves edges and labels; i.e.

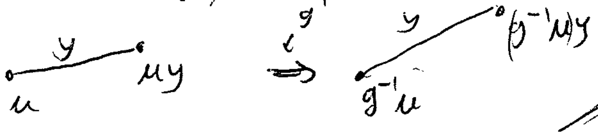


don't change the label!

Looking again at $C(X,R)$; if $g \in G$, define $g' : G \to G$ by $g' : x \mapsto g^{-1}x$

In fact, g' is an automorphism of $C(X,R)$:

Let $u \in G$, $y \in X \cup X^{-1}$



We have then that $g \mapsto g'$ is an homomorphism $G \to \mathrm{Aut}(C(X,R))$.

In fact, it is an iso:

Suppose $\alpha \in \mathrm{Aut}\, C(X,R)$. Then $(uy)\alpha = (u)\alpha \cdot y$.

Put $u = 1$: $(y)\alpha = (1)\alpha \cdot y \Rightarrow \alpha = \left(((1)\alpha)^{-1}\right)'$ $\Rightarrow$ surjective.

It's clearly injective, so ✓.

We've proven:

<u>Prop</u>: $G \cong \mathrm{Aut}(C(X,R))$

• Verbal subgroups and group varieties.

Let F be a free group on a countably infinite set $\{x_1, x_2, \dots\}$.

Let $w \in F$, so w is a reduced word in $x_1, x_2, \dots$. Suppose $w = w(x_1, \dots, x_r)$.

Let G be any group, and choose $g_1, \dots g_r \in G$.

Def: The *value* of w at $(g_1, \dots, g_r)$ is $w(g_1, g_2, \dots, g_r) \overset{= w(\underline{g})}{\in} G$.

Def: Let $\emptyset \neq W \subseteq F$. The *verbal subgroup of G corresponding to W* is $W(G) := \langle w(\underline{g}) : w \in W, g_i \in G \rangle$

$W(G)$ is *fully invariant* in G (i.e. $\alpha : G \to G$ is an endomorphism, then $W(G)^{\alpha} \subseteq W(G)$).

$(w(g_1, \dots, g_r)^{\alpha} = w(g_1^{\alpha}, \dots, g_r^{\alpha}) \in W(G))$.

In particular, $W(G) \triangleleft G$.

Conversely, for free groups we have:

Thm (BH Neumann): If F is a free group, and H is a fully invariant subgroup of F, then H is a verbal subgroup.

Pf Let F be free on X.

Let $w \in H$. So $w = w(\underline{x}) = w(x_1, \dots, x_r)$, $x_i \in X$. Let $f_1, \dots, f_r \in F$.

Need to show that $w(\underline{f}) \in H$.

There is a homomorphism $\alpha : F \to F$ s.t. $\begin{cases} x_i \mapsto f_i & 1 \le i \le r \\ x_j \mapsto 1 & \text{if } x_j \in X \setminus \{x_1, \dots, x_r\} \end{cases}$ (by univ. ppty)

Then, $w^{\alpha} = w(\underline{f}) \in H$ since H is fully invariant.

Hence, H is verbal,

Example: Let G be of type $p^{\infty} = \bigcup \mu_{p^n}$. It has a unique subgroup of order p, call it H. So H is fully invariant in G. But H is not verbal.

(exercise).

Examples:

1) $W = \{[x_1, x_2]\}$. Then $W(G) = G'$.

2) $W = \{[x_1, \ldots, x_c]\}$. Then $W(G) = \gamma_c(G)$

3) $W = \{x_1^n\}$. Then $W(G) = G^n$ (generated by all n^{th}-powers)

4) $W = \{[[x_1, x_2], [x_3, x_4]]\} \Rightarrow W(G) = G''$ ← and could do for any $G^{(i)}$!

Varieties of groups.

Def Let W be a set of words in $\{x_1, x_2, \ldots\}$. Then the variety of groups determined by W is the class of groups $\{G \mid W(G) = 1\} =: Var(W)$

Examples:

1) $W = \{[x_1, x_2]\} \rightarrow Var(W) =$ abelian groups.

2) $W = \{[x_1, \ldots, x_{c+1}]\} \rightarrow Var(W) =$ nilpotent groups of class $\leq c$.

3) $W = \{x_1^n\}$. $Var(W)$ is the Burnside variety: G s.t. $g^n = 1$ $\forall g \in G$.

Note: The class of nilpotent groups is not a variety.
(every variety is closed under forming unrestricted direct products).

Relatively free groups

Let $\underline{V} = Var(W)$ be a variety.

Then, $\underline{V}$, together with all homomorphisms between free groups, is a category.

In fact, $\underline{V}$ contains free objects.

↓

Theorem: Let W be a set of words, and let F be a free group on a set X. Let $\underline{\underline{V}} = Var(W)$. Then $\bar{F} := F/_{W(F)}$ is a free object in $\underline{\underline{V}}$.

~~Pf~~ Let $G \in \underline{\underline{V}}$, let $\alpha : X \to G$ be any map. Let (F, σ) be free on X. $\sigma : X \to F$. Applying the mapping property to F, calling $\nu : F \to \bar{F}$ the canonical map, get $\beta : F \to G$. Composing $\sigma\nu$, get $\sigma\nu : X \to \bar{F}$.

$$\begin{tikzcd} & F \arrow[d] \arrow[ddr, "\beta"] & \\ & \bar{F} & \\ X \arrow[uur, "\sigma"] \arrow[ur, dashed, "\sigma\nu"] \arrow[rr, "\alpha"'] & & G \end{tikzcd}$$

Define $\theta : \bar{F} \to G$ by $\left(f W(F)\right)^{\theta} := f^{\beta}$.

It is well defined, because $(W(F))^{\beta} = W(F^{\beta}) \subseteq W(G) = 1$ since $G \in \underline{\underline{V}} = Var(W)$.

Note that $\sigma\nu\theta = \sigma\beta = \alpha \Rightarrow$ lower triangle commutes $\Rightarrow$ ✓.

If $\theta' : \bar{F} \to G$ is another hom. making it commute $(\sigma\nu\theta' = \alpha)$,

then $\sigma\nu\theta' = \sigma\nu\theta \Rightarrow \theta = \theta'$, because $\langle \mathrm{Im}\, \sigma\nu \rangle = \bar{F}$.

//

Theorem: Every group in $\underline{\underline{V}} = Var(W)$ is isomorphic with a quotient group of some free group in $\underline{\underline{V}}$ (call them free $\underline{\underline{V}}$-groups).

~~Pf~~ Let $G = \langle X \rangle \in \underline{\underline{V}}$. Let F be free on X. Let $\bar{F} := F/_{W(F)}$ (if $\underline{\underline{V}} = Var(W)$). Then $\bar{F}$ is free on $\underline{\underline{V}}$, and so the mapping property gives a hom. from $\bar{F} \to G$. But it is surjective, because $G = \langle X \rangle$.

//

Example: Let $\underline{\underline{V}}$ = class of nilpotent groups of class $\leq c$. So $\underline{\underline{V}}$ is determined by $\{[x_1, \ldots, x_{c+1}]\}$. So a ~~free~~ group in $\underline{\underline{V}}$ has the form $F/_{\gamma_{c+1}(F)}$, where F is free.

Therefore, every nilpotent of class $\leq c$ is isomorphic with a quotient group of some $F/_{\gamma_{c+1}(F)}$, with F free.

§ 7. Subgroups of Free Groups.

Thm (The Nielsen - Schreier Theorem)

Let W be a subgroup of a free group F. Then W is a free group; and if $m = |F:W|$ is finite and F has rank n (possibly ∞), then W has rank $mn + 1 - m$

Pf/ We'll follow the algebraic approach (as opposed to Serre's approach, using trees).

Let F be free on a set X. Let the right cosets of W in F be $\{W_i \mid i \in I\}$, where we assume $W = W_1$.

Choose an element $\overline{W_i}$ from W_i. Then $\{\overline{W_i} \mid i \in I\}$ is a right transversal to W in F, and choose $\overline{W_1} (= \overline{W} =) 1$. Also, note that $W_i = W\overline{W_i}$.

If $u \in F$, then $\overline{W_i} u$ and $\overline{W_i u}$ belong to the same coset $W_i u$.

Hence, $\overline{W_i} u \overline{W_i u}^{-1} \in W$.

The idea is to choose the $\overline{W_i}$ in such a way that the non-trivial elements $\overline{W_i} u \overline{W_i u}^{-1}$ freely generate W.

For each $i \in I$, $x \in X$, consider the symbol y_{ix}, and define $\hat{F}$ to be the free group on the set $\{y_{ix} \mid i \in I, x \in X\}$.

Define a hom. $\tau : \hat{F} \to W$ by the rule $y_{ix}^{\tau} = \overline{W_i} \, x \, \overline{W_i x}^{-1}$.

- $\underline{\tau \text{ is surjective}}$ (by the idea of $\underline{\text{Coset Maps}}$)

Let $u \in F$, $i \in I$. Define an element $u^{W_i} \in \hat{F}$ as follows:

$1^{W_i} = 1$, $x^{W_i} = y_{ix}$, $(x^{-1})^{W_i} = (x^{W_i x^{-1}})^{-1}$. Now, complete the definition by recursion on the length of the reduced word:

If $u = vy$, $v \in F$, $y \in X \cup X^{-1}$, in reduced form. Define $u^{W_i} := (v^{W_i}) y^{W_i v}$.

$u \mapsto u^{W_i}$ is called a $\underline{\text{coset map}}$, from $F \to \hat{F}$.

↓

47

(cont pf of N-S thm).

We need a lemma:

Lemma: For any $u, v \in F, i \in I$:

(i) $(uv)^{W_i} = u^{W_i} v^{W_i u}$

(ii) $(u^{-1})^{W_i} = \left(u^{W_i u^{-1}}\right)^{-1}$

Pf/

(i) If $v = 1$, clearly true.

Induct on the length of v as a reduced word.

Suppose $v \in X \cup X^{-1}$.

If the final syllable of u is not v^{-1}, it follows by definition.

Suppose now that u ends on v^{-1}: so $u = u_1 v^{-1} \Rightarrow uv = u_1$.

Then $u^{W_i} = (u_1 v^{-1})^{W_i} = u_1^{W_i} (v^{-1})^{W_i u_1} = u_1^{W_i} \left(v^{W_i u_1 v^{-1}}\right)^{-1}$

$\therefore u^{W_i} = u_1^{W_i} \cdot \left(v^{W_i u}\right)^{-1} \Rightarrow u_1^{W_i} = u^{W_i} \cdot v^{W_i u}$ $\Rightarrow (uv)^{W_i} = u^{W_i} v^{W_i u}$ //

(ii) Now assume that v has length > 1. Write $v = v_1 y$ (~~reduced~~ form), and $y \in X \cup X^{-1}$.

Then, $(uv)^{W_i} = (u v_1 y)^{W_i} = (u v_1)^{W_i} y^{W_i u v_1} = u^{W_i} v_1^{W_i u} y^{W_i u v_1} = u^{W_i} (v_1 y)^{W_i u}$ //

(ii) $1 = 1^{W_i} = (u^{-1} u)^{W_i} = (u^{-1})^{W_i} u^{W_i u^{-1}} \Rightarrow (u^{-1})^{W_i} = \left(u^{W_i u^{-1}}\right)^{-1}$ //

Continuing with the proof, we compose $u \mapsto u^{W_i}$ and $\tau : \hat{F} \to W$:

Lemma 2: For any $u \in F$, $i \in I$,

$$\left(u^{W_i}\right)^{\tau} = \overline{W_i}\, u \left(\overline{W_i u}\right)^{-1}$$

Pf/ Induct on the length of u as a reduced word (if $u = 1$, clear). If $u \in X \cup X^{-1}$, it follows from the definition.

Let u have length > 1, and write $u = u_1 \overset{\text{reduced}}{v}$, $v \in X \cup X^{-1}$.

$$\left(u^{W_i}\right)^{\tau} = \left((u_1 v)^{W_i}\right)^{\tau} = \left(u_1^{W_i} v^{W_i u_1}\right)^{\tau} = \left(u_1^{W_i}\right)^{\tau} \left(v^{W_i u_1}\right)^{\tau} \overset{\text{ind. hyp}}{=} \overline{W_i}\, u_1 \left(\overline{W_i u_1}\right)^{-1} \cdot \cancel{\overline{W_i u_1}} \cdot v \cdot \overline{W_i u_1 v}^{-1}$$

$$= \overline{W_i}\, u\, \overline{W_i u}^{-1}.$$ //

(cont pf).

Next, we look at the restriction of $u \mapsto u^W$ to W. (i.e $u \in W$).

This restriction is a map $\psi : W \to \hat{F}$.

If $u, v \in W$, $(uv)^{\psi} = (uv)^W = u^W v^{W_u} = u^W v^W \Rightarrow \psi$ is a homomorphism.

For $u \in W$,

$u^{\psi\tau} = (u^W)^{\tau} = \overline{W} u \overline{Wu}^{-1} = 1 u 1 = u \Rightarrow \psi\tau$ is the identity on W.

Hence, ψ is injective, and $\tau : \hat{F} \to W$ is surjective $\Rightarrow \tau : \hat{F} \to W$ is a presentation.

Put $\chi := \tau\psi : \hat{F} \to \hat{F}$. $\chi \in End(\hat{F})$. Note that $\chi^2 = \tau \boxed{\overset{1}{\psi\tau}} \psi = \tau\psi = \chi$.

This is called a retraction $(\chi^2 = \chi)$.

Lemma 3: The group W has the presentation given by $\tau : \hat{F} \to W$ in generators y_{ix}'s with ~~the~~ defining relators:

$$y_{ix}^{-1} y_{ix}^{\chi} \qquad (i \in I, x \in X)$$

Pf Define $N := \langle y_{ix}^{-1} y_{ix}^{\chi} \mid i \in I, x \in X \rangle^{\hat{F}}$ (normal closure in $\hat{F}$).

Will show that $N = Ker(\tau) =: K$. (note that $K = Ker\ \tau \circ \psi = Ker\ \chi$, as ψ is injective).

Firstly, $(y_{ix}^{-1} y_{ix}^{\chi})^{\chi} = (y_{ix}^{-1})^{\chi} y_{ix}^{\chi^2 = \chi} = 1 \Rightarrow N \leq K$.

Let now $k \in K$.

$$y_{ix}^{\chi} \equiv y_{ix} \pmod N$$

Hence, $1 = k^{\chi} \equiv k \pmod N \Rightarrow k \in N \Rightarrow K = N$.

Next, we get a more convenient set of defining relators.

Lemma 4:

The elements u^W, where u is a non-trivial transversal element, form a set of defining relators for the presentation $\tau : \hat{F} \to W$.

Pf If u is a transversal element, then $\overline{Wu} = u$. So $(u^W)^{\tau} = \overline{W} u \overline{Wu}^{-1} = 1 u u^{-1} = 1$.

Hence $u^W \in K = Ker\ \tau = Ker\ \chi$.

↓

(48)

(Cont pf)

Put $N = \langle u^{w} \mid u \text{ a transversal elt} \rangle^{\hat{F}}$. Then $N \leq K$. To prove the converse, its enough to show that $y_{ix}^{-1} y_{ix}^{x} \in N$ (for then $K \leq N$).

$$y_{ix}^{x} = \left(y_{ix}^{\tau}\right)^{W} \underset{\substack{\uparrow \\ \text{def of } \tau}}{=} \left(\overline{W_i} x \overline{W_i x}^{-1}\right)^{W} = \overline{W_i}^{W} x^{W\overline{W_i}} \left(\overline{W_i x}^{-1}\right)^{W\overline{W_i x}} = \overline{W_i}^{W} x^{W\overline{W_i}} \left(\left(\overline{W_i x}\right)^{(W\overline{W_i x})(\overline{W_i x})^{-1}}\right)^{-1} =$$

$$= \overline{W_i}^{W} x^{W_i} \left(\overline{W_i x}^{W}\right)^{-1} \equiv x^{W_i} \pmod N = y_{ix} \pmod N$$

$$\Rightarrow y_{ix}^{x} \equiv y_{ix} \pmod N \quad \Rightarrow \quad y_{ix}^{-1} y_{ix}^{x} \in N.$$

//

Now, we choose what is called a <u>Schreier's transversal</u>:

Schreier Transversals

Let $\emptyset \neq S \subseteq F$. Call S a Schreier subset if $\left.\begin{array}{l} vy \in S \\ \text{reduced} \\ y \in X \cup X^{-1} \end{array}\right\} \Rightarrow v \in S$

Examples:

Let $x_1, x_2 \in X$. Then $S := \{ x_1^{n_1} x_2^{n_2} \mid n_1, n_2 \geq 0 \}$ is a Schreier subset.

~~Also~~, However, $\{ x_2, x_1 x_2 \}$ is not (as $x_1 \notin$ it).

Lemma 5: There is a right transversal to W in F which is a Schreier subset.

~~Pf~~ Define the length of a coset W_i to be the length of the shortest element in W_i (in reduced form).

Note that the only coset with length 0 is W. Choose $\overline{W} = 1$.

Assume that $\overline{W_i}$, rep' for W_i has been assigned for all cosets W_i with length $< \ell$ ($\ell \geq 1$), such that this set has the Schreier property.

Suppose that W_i has length ℓ. $\Rightarrow \exists u \in W_i$, where u has length ℓ (in reduced form).

Write $u = vy$, $y \in X \cup X^{-1}$ in ~~reduced~~ form. Then v has length $\ell - 1$.

So Wv has length $\ell - 1 \Rightarrow \overline{Wv}$ has been assigned. Define then $\overline{W_i} := (\overline{Wv}) y$.

//

Proof of the Nielsen-Schreier Theorem: (until here, have been setting the stage).

Choose a Schreier transversal $\overline{W_i}$ to W in F.

Let $K := \ker(\tau)$, where $\tau : \hat{F} \to W$, $y_{ix}^{\tau} = \overline{W_i} x \overline{W_i x}^{-1}$.

Recall that $K = \ker(\chi)$, and K is the normal closure in $\hat{F}$ of all the u^W where u is a nontrivial transversal element.

Let u be such a transversal element, $u \neq 1$. Write $u = vx^{\varepsilon}$ $(x \in X, \varepsilon = \pm 1)$.

By the Schreier property, v is also a transversal element.

Now, $u^W = (vx^{\varepsilon})^W = v^W (x^{\varepsilon})^{Wv}$.

If $\varepsilon = 1$, get $u = vx \Rightarrow u^W = v^W x^{Wv} = v^W x^{W_k}$ $\quad (W_k := Wv)$. $= v^W y_{xk}$.

Now, $u^W, v^W \in K \Rightarrow y_{xk} \in K$.

If $\varepsilon = -1$, $u = vx^{-1} \Rightarrow u^W = (vx^{-1})^W = v^W (x^{-1})^{Wv} = v^W \big(x^{\overset{Wvx^{-1} = Wu =: W_\ell}{\overbrace{Wvx^{-1}}}}\big)^{-1} = v^W y_{x\ell}^{-1}$.

So get $y_{x\ell} \in K$

By repeating this argument, we can express the original u^W in terms of certain $y_{\kappa x}$'s, which lie in K.

Conclusion: K is the normal closure in $\hat{F}$ of certain of the $y_{\kappa x}$'s.

So just need to prove the following lemma:

Lemma: Let $\emptyset \neq Y \subseteq X$, F free on X. Then F/Y^F is free on $X \setminus Y$. (exercise).

Hence, W is free on the set of y_{ix}'s that are not killed by τ.

Now, assume that $|F : W| = m < \infty$, and $\operatorname{rank}(F) = n \ (\leq) \infty$.

Then $\operatorname{rk} \hat{F} = mn$ ($\hat{F}$ is free on the y_{ix}'s).

We need to show that exactly $m-1$ y_{ix}'s are in K (so that W is free with $\operatorname{rk} = mn - m + 1$).

Now, $y_{ix} \in K \Leftrightarrow y_{ix}^{\tau} = 1 \Leftrightarrow \overline{W_i} x = \overline{W_i x}$.

Choose any $W_i \neq W$ (have $m-1$ choices), and let x^{ε} be the final symbol of $\overline{W_i}$.

Say $W_j := W_i (x^{\varepsilon})^{-1}$. Then $\overline{W_i} = \overline{W_j} x^{\varepsilon}$. By the Schreier property,

$\Downarrow$

(cont pf).

Got that $\overline{W_i} = \overline{W_j x^{\varepsilon}}$.

<u>If $\varepsilon = 1$</u>, then we have $W_i = W_j x$, and $\overline{W_j}\, x\, \overline{W_j x}^{-1} = \overline{W_j}\, x\, \overline{W_i}^{-1} = 1$

Hence $y_{jx}^{\tau} = 1 \Rightarrow y_{jx} \in K$.

<u>If $\varepsilon = -1$</u>, then we have $W_i x = W_j$. and $\overline{W_i}\, x\, \overline{W_i x}^{-1} = \overline{W_i}\, x\, \overline{W_j}^{-1} = 1$

Hence, $y_{ix}^{\tau} = 1 \Rightarrow y_{ix} \in K$.

So each coset other than W gives (at least) one of the y_{ix}'s in K.

Conversely, suppose that $y_{ix} \in K$. Then $\overline{W_i}\, x\, \overline{W_i x}^{-1} = 1$.

Let $W_j := W_i x$. Thus, $\overline{W_i}\, x\, \overline{W_j}^{-1} = 1$.

Either $W_i \neq W$ or $W_j \neq W$ (otherwise $x = 1$!). Can show that y_{ix} comes from either W_i or W_j.

<u>Conclusion</u>: all y_{ix}'s in K are in one of the cosets $\Rightarrow$ $n-1$ of them.

End of pf of N-S.

<u>Application</u>:

<u>Theorem</u>: Let F be a free group with $\operatorname{rk} F \geq 2$. Then F' is free, with infinite rank.

Pf Let F be free on ~~$\{x_1, x_2, \ldots, x_2$~~ X, which we assume to be ordered

Put $S = \{ x_1^{l_1} x_2^{l_2} \cdots x_r^{l_r} \mid x_i$ distinct elements of X, all $l_i \neq 0 \}$ (as F/F' is free abelian on $x_i F'$).

S is a right transversal with the Schreier property.

Let $W_i = W x_2^{l_2}$ $(l_2 > 0)$ (we set $W := F'$).

Then, $y_{ix_1}^{\tau} = \overline{W_i}\, x_1\, \overline{W_i x_1}^{-1}$. As $W_i x_1 = W x_2^{l_2} x_1 = W x_1 x_2^{l_2}$, then $\overline{W_i x_1} = x_1 x_2^{l_2}$

get $y_{ix_1}^{\tau} = x_2^{l_2} x_1 (x_1 x_2^{l_2})^{-1} = x_2^{l_2} x_1 x_2^{-l_2} x_1^{-1} \neq 1$

So there are infinitely many free generators for F'.

Presentations of subgroups

Thm (Reidemeister - Schreier):
Let G be a group with a presentation given by $\varphi : F \to G$, F free on X,
say $G = \langle X \mid S \rangle$. Let $H \leqslant G$ be a subgroup.
Let $\tau, \hat{F}$ be as in Nielsen-Schreier proof, and let $W :=$ preimage of H under φ, $W \leqslant F$.
Then: $\tau\varphi : \hat{F} \longrightarrow H$ is a surjective homomorphism, giving a presentation of H in y_{ix}'s ($i \in I$, $x \in X$), with relators s^{W_i}, u^W, where $s \in S$, $u \neq 1$ is a transversal element (to W in F).

Proof: $\tau\varphi$ is the composition of two surjectives, hence it's surjective.

$\ker(\tau\varphi) =$ preimage of $K = \ker(\varphi)$ under τ.

Put $N := \langle s^{W_i}, u^W \mid i \in I,\ s \in S,\ 1 \neq u \text{ transversal} \rangle^{\hat{F}}$.

Want to show that $N = \ker(\tau\varphi)$.

Note that $S \subseteq K \leqslant W$. Also, $K \triangleleft F$ (K is a kernel).

Also, $W_i s = W_i$, because $Wus = Ws^{u^{-1}}u = Wu$ since $s^{u^{-1}} \in K \leqslant W$.

Therefore, $(s^{W_i})^{\tau} = \overline{W_i}\, s\, \overline{W_i s}^{-1} = \overline{W_i}\, s\, \overline{W_i}^{-1} = s^{(\overline{W_i}^{-1})}$.

Then, $N^{\tau} = \langle \underbrace{(u^W)^{\tau}}_{= 1}, (s^{W_i})^{\tau} \rangle^W = \langle \overline{W_i}\, s\, \overline{W_i}^{-1} : s \in S,\ i \in I \rangle^W = S^F = \underset{(\ker\varphi)}{K}$

Recall that $W = \varphi^{-1}(H)$. Hence, $\ker(\tau\varphi) = N \cdot (\ker\tau) = N$

(since $\ker\tau = \langle u^W \mid u \text{ transversal} \rangle^{\hat{F}} \subseteq N$)

So the s^{W_i}, u^W form defining relations for H.

Theorem (Iwasawa): Let F be any free group, and p any prime. Then, F is a residually (finite p) group.

(G is residually $\mathcal{P}$ if given $1 \neq g \in G$, $\exists N \triangleleft G$, $g \notin N$ s.t. G/N is $\mathcal{P}$).

Pf/ Let F be free on a set X, let $1 \neq f \in F$. We will prove that there's a homomorphism $\theta : F \to \underset{p\text{-group}}{\text{some finite}}$ s.t. $f^\theta \neq 1$. Then, $G/\ker\theta \cong$ finite p group and, since $f^\theta \neq 1$, $f \notin \ker\theta$.

Write $f = x_{i_1}^{m_1} \cdots x_{i_r}^{m_r}$ $\left(x_{i_j} \in X,\ m_i \neq 0,\ x_{i_j} \neq x_{i_{j+1}} \right)$

Write $q := \max\{i_1, .., i_r\}$.

Recall (or define) E_{kl} for the $(r+1)\times(r+1)$ matrix whose kl entry is 1, the others 0, considered as a matrix over $\mathbb{Z}/p^n\mathbb{Z}$, where $p^n \nmid m_1 m_2 \cdots m_r$

Write $\mathcal{U} := U_{r+1}(\mathbb{Z}/p^n\mathbb{Z})$ (unitriangular group). $\#\mathcal{U} = p^{n\binom{r+1}{2}}$ $\Leftarrow$ a finite p-group.

Note that $1 + E_{kl} \in \mathcal{U}$ if $k < l$.

Define $\underset{(j=1 \cdots q)}{g_j \in \mathcal{U}}$ by $g_j := \prod_{i_u = j} (1 + E_{u,u+1}) \in \mathcal{U}$. ($g_j = 1$ if $i_u \neq j$ $\forall u$).

Note that the factors of the product commute, because $\begin{cases} E_{kl} E_{lm} = E_{km} \\ E_{kl} E_{l_1 m} = 0 \text{ if } l \neq l_1 \end{cases}$ and because $i_j \neq i_{j+1}$.

Since F is free on X, we can define a homomorphism $\theta : F \to \mathcal{U}$ by $x_{i_u}^\theta := g_{i_u}$ and for all the other x, $x^\theta := 1$. This is a hom. because F is free, and $f^\theta \neq 1$: $f^\theta = g_{i_1}^{m_1} \cdots g_{i_r}^{m_r}$.

Now note that $g_j := \prod_{i_u = j} (1 + E_{u,u+1}) \overset{\text{since } i_u \neq i_{u+1}}{=} 1 + \sum_{i_u = j} E_{u,u+1}$, and $g_j^l = 1 + l \cdot \sum_{i_u = j} E_{u,u+1}$.

Hence, $f^\theta = \left(1 + m_1 \sum_{i_1 = i_u} E_{u,u+1}\right) \cdots\cdots \left(1 + m_r \sum_{i_r = i_u} E_{u,u+1}\right) = 1 + \overbrace{(m_1 m_2 \cdots m_r) \cdot E_{12} E_{23} E_{34} \cdots E_{r,r+1}}^{= E_{1,r+1}} + \cdots$

as $p^n \nmid m_1 \cdots m_r$, this is not trivial.

//

Corollary (Magnus):

If F is any free group, then $\bigcap_{i\geq 1} \gamma_i(F) = 1$ (lower central chain).

So F is residually-nilpotent.

This implies that F can be embedded in the unrestricted free product of $F/\gamma_i(F)$.

Pf/ If $N \lhd F$, F/N a finite p-group, then F/N is nilpotent, so $\gamma_{c+1}(F) \leq N$ for some c. As $\bigcap_N N = 1$, we're done. //

Corollary: Also, $\bigcap_{i\geq 1} F^{(i)} = 1$, because $F^{(i)} \leq \gamma_{2^i}(F)$

§8. Free Products.

In the category Grp, the product of a set $\{G_\lambda : \lambda \in \Lambda\}$ is the cartesian product (or the unrestricted direct product) $\prod_\lambda G_\lambda$.

What is (if exists) the coproduct?

Formally, a coproduct of $\{G_\lambda : \lambda \in \Lambda\}$ in Gp is a group G and a collection of homomorphisms $i_\lambda : G_\lambda \to G$ s.t they have the mapping property: given homs $\varphi_\lambda : G_\lambda \to H$ (H some gp). Then $\exists!$ homomorphism $\varphi : G \to H$, s.t. $i_\lambda \varphi = \varphi_\lambda$ $\forall \lambda \in A$

$$\begin{tikzcd} G_\lambda \arrow[r, "i_\lambda"] \arrow[dr, "\varphi_\lambda"'] & G \arrow[d, "\exists! \varphi"] \\ & H \end{tikzcd}$$

(if exists, then unique upto unique ~~iso~~)

For example, suppose we have a group J generated by subgroups G_λ, $\lambda \in \Lambda$. Let $\varphi_\lambda : G_\lambda \to J$ be the inclusion. Hence $\exists!$ homo. $\varphi : G \to J$. Note that then φ needs to be surjective (because J is generated by the G_λ). In some sense, G should be the "largest" group that can be generated by G_λ's.

We call such a coproduct the free product of $\{G_\lambda\}$.

Theorem: Let $\{G_\lambda\}_{\lambda\in\Lambda}$ be any non-empty set of groups. Then a free product of $\{G_\lambda\}$ exists.

Pf/ We will construct such thing.

We can assume that $G_\lambda \cap G_\mu = \emptyset$ if $\lambda \neq \mu$ (by replacing, if necessary, some of the G_λ by suitable isomorphic copies).

Consider now S ~~to~~ be the set of all words in $\dot{\bigcup}_{\lambda\in\Lambda} G_\lambda$, i.e. finite sequences of elements of G_λ: $g = g_1 g_2 \cdots g_r$, $g_i \in G_{\lambda_i}$, $\lambda_i \in \Lambda$.

We allow the empty word 1.

Form the product of two words g, h by juxtaposition, with $1g = g1 = g$.

Then S is a monoid.

Now we introduce a relation on S, $\sim$:

$g \sim h$ if one can pass from g to h by a finite number of operations of the following types:

(i) Insertion or deletion some identity element 1_{G_λ}.

(ii) Replacement of two consecutive elements of the word in the same G_λ by their product $\cdots g_i g_j \cdots \longrightarrow \cdots (g_i g_j) \cdots$ or the reverse operation.

Then $\sim$ is an equivalence relation on S. Write $[g]$ for the equ. class of $g \in S$.

Define $G := \{[g] \mid g \in S\}$, and a group operation: $[g][h] := [gh]$.

Note that $g \sim g'$, $h \sim g'$ then $[gh] = [g'h']$. ($\Rightarrow$ gp op. well-defined).

Define also, if $g = g_1 \cdots g_r$, $g^{-1} = g_r^{-1} \cdots g_1^{-1}$.

G becomes a group, with $[1]$ its identity, and $[g]^{-1} = [g^{-1}]$.

Define the maps $i_\lambda : G_\lambda \to G$ by, if $x \in G_\lambda$, $x^{i_\lambda} := [x]$.

Check that i_λ are gp homomorphisms, but need to check now the mapping property.

↓

Now we check the coproduct property: let $\{\varphi_\lambda : G_\lambda \to H\}$ be a family of homs into H.

Define $\varphi : G \longrightarrow H$ by, $[g] \in G$, $g \in S$, $g = g_1 \cdots g_r$, $g_i \in G_{\lambda_i}$,

$$[g]^\varphi = g_1^{\varphi_{\lambda_1}} \cdots\cdots g_r^{\varphi_{\lambda_r}} \in H.$$

The hom. φ is well defined, since by applying the operations of Types (1), (2) don't make any difference (and is a homomorphism, by how it's defined).

$$\begin{tikzcd} G_\lambda \arrow[rr, "i_\lambda"] \arrow[dr, "\varphi_\lambda"'] & \circlearrowright & G \arrow[dl, "\varphi"] \\ & H & \end{tikzcd}$$

$\forall \lambda$, let $x \in G_\lambda$. Then

$$x^{i_\lambda \varphi} = [x]^\varphi = x^{\varphi_\lambda} \Rightarrow i_\lambda \varphi = \varphi_\lambda .$$

Suppose now that $\varphi' : G \longrightarrow H$ is another hom. making the triangle commute.

Then φ and φ' agree on the image of i_λ, $\operatorname{Im} i_\lambda \subseteq G$.

But $\langle \operatorname{Im}(i_\lambda) \mid \lambda \in \Lambda \rangle = G$ because if $g = g_1 \cdots g_r$, then

$[g] = [g_1] \cdots [g_r]$, and $[g_i] = i_{\lambda_i}(g_i)$. $\Rightarrow$ φ is unique.

Hence $(G, \{i_\lambda\})$ is the coproduct in Gp. //

Notation for free products

We write $\underset{\lambda \in \Lambda}{\mathrm{Fr}}\, G_\lambda$ for the free product of $\{G_\lambda\}_{\lambda \in \Lambda}$.

But if $\Lambda = \{1, 2, \ldots, n\}$ we write $G_1 * G_2 * \cdots * G_n$ for the free product

Rk: if each $G_\lambda = \langle g_\lambda \rangle \simeq \mathbb{Z}$ $\forall \lambda \in \Lambda$, then $\underset{\lambda}{\mathrm{Fr}}\, G_\lambda$ is free on $\{g_\lambda \mid \lambda \in \Lambda\}$.

Reduced words and Normal form in free products.

Let $G = \underset{\lambda \in \Lambda}{\mathrm{Fr}}\, G_\lambda$, just constructed.

Def A word in $\bigcup_\lambda G_\lambda$ $(g = g_1 \cdots g_r)$ is called <u>reduced</u> if it contains no identity elements, and if g_i, g_{i+1} belong to different G_λ's $(\forall i)$. $(\lambda_i \neq \lambda_{i+1})$.

The empty word is considered reduced.

Clearly, every equivalence class contains a reduced word.

How we prove that there is only <u>one</u> reduced word in each class?

<u>Theorem</u>: Each equivalence class of words in $\bigcup G_\lambda$ contains a unique reduced word.

Pf Suppose g, h are two equivalent reduced words. Want to show $g = h$.

Introduce the set R of <u>all</u> reduced words in $\bigcup_\lambda G_\lambda$.

Let $u \in G_\lambda$, and define $u' \in \mathrm{Sym}(R)$ as follows:

- if $u = 1_{G_\lambda}$, then $u' = 1_{\mathrm{Sym}(R)}$.
- if $u \neq 1_{G_\lambda}$, and $x_1 x_2 \cdots x_r \in R$ $(x_i \in G_{\lambda_i}$, then

$$(x_1 \cdots x_r)u' = \begin{cases} x_1 \cdots x_r u & \text{if } \lambda_r \neq \lambda \\ x_1 \cdots x_{r-1}(x_r u) & \lambda_r = \lambda,\ x_r u \neq 1 \\ x_1 \cdots x_{r-1} & \lambda_r = \lambda, x_r u = 1 \end{cases}$$

(note that $(u')^{-1} = (u^{-1})'$, so $u' \in \mathrm{Sym}(R)$).

Let $\varphi_\lambda : G_\lambda \to \mathrm{Sym}(R)$ be $u \mapsto u'$ $(u \in G_\lambda)$.

$$\begin{tikzcd} G_\lambda \arrow[r, "i_\lambda"] \arrow[dr, "\varphi_\lambda"'] & G \arrow[d, dashed, "\varphi"] \\ & \mathrm{Sym}(R) \end{tikzcd}$$

s.t. $i_\lambda \varphi = \varphi_\lambda$ $\forall \lambda$.

Write $g = y_1 \cdots y_s$, $y_i \in G_{\lambda_i}$, $\lambda_i \in \Lambda$. Then $[y] = [y_1] \cdots [y_s]$,

and $[g]^\varphi = [y_1]^\varphi \cdots [y_s]^\varphi = y_1^{i_{\lambda_1}\varphi} \cdots y_s^{i_{\lambda_s}\varphi} = y_1^{\varphi_{\lambda_1}} \cdots y_s^{\varphi_{\lambda_s}} = y_1' \cdots y_s'$.

Hence, $[g]^\varphi$ sends 1 to $(1) y_1' \cdots y_s' = y_1 \cdots y_s = g$.

But $[g] = [h]$, then $g = h$

Let now $[g] \in \underset{\lambda\in\Lambda}{\mathrm{Fr}}\, G_\lambda$, where g is the unique reduced word in $[g]$.

Then, $g = g_1 g_2 \cdots g_r$, so $g_i \in G_{\lambda_i}$ ($\lambda_i \in \Lambda$). Here, $\lambda_i \neq \lambda_{i+1}$, and $g_i \neq 1_{G_{\lambda_i}}$, $r \geq 0$.

This is a normal form in $\underset{\lambda\in\Lambda}{\mathrm{Fr}}\, G_\lambda$.

Conversely

Theorem: Let G be a group, and let $\{G_\lambda\}_{\lambda\in\Lambda}$ be a collection of subgroups of G, such that each element $g \in G$ has a unique expression as

$$g = g_1 g_2 \cdots g_r, \quad g_i \in G_{\lambda_i} \ (\lambda_i \in \Lambda), \quad g_i \neq 1, \quad \lambda_i \neq \lambda_{i+1}, \quad r \geq 0.$$

Then: $G \cong \underset{\lambda\in\Lambda}{\mathrm{Fr}}\, G_\lambda$.

Pf/ Apply the mapping property of the coproduct to $G_\lambda \overset{i}{\hookrightarrow} G$.

Get an hom. $\theta : \mathrm{Fr}\, G_\lambda \to G$, which is surjective since $G = \langle G_\lambda \mid \lambda \in \Lambda \rangle$.

Suppose $[g] \in \mathrm{Fr}\, G_\lambda$, $g = g_1 \cdots g_r$ in normal form.

Then $[g]^\theta = g_1 \cdots g_r$ in G. If $[g]^\theta = 1$, then $g_1 \cdots g_r = 1$.

As the g was already in normal form, it has to be the empty word. //

Examples:

1. If $G_\lambda \simeq \mathbb{Z}$, then $\underset{\lambda\in\Lambda}{\mathrm{Fr}}\, G_\lambda$ is a free group on Λ (follows from the mapping property).
2. Let $G = \langle x \rangle$, $H = \langle y \rangle$, of order 2 each. Then $G * H = \langle x, y \mid x^2, y^2 \rangle = \mathrm{Dih}(\infty)$.
3. $PSL_2(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ (Fuche & Klen).

Pf/

Recall $SL_2(\mathbb{Z}) = \{A \in GL_2(\mathbb{Z}), \det A = 1\}$. $Z(SL_2(\mathbb{Z})) = \{\pm 1_2\}$. $PSL_2(\mathbb{Z}) = \dfrac{SL_2(\mathbb{Z})}{\{\pm 1\}}$

Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$.

Note that $A^2 = -I$, $B^3 = -I$.

Define $H := \langle A, B \rangle \leq SL_2(\mathbb{Z})$. To show that actually $H = SL_2(\mathbb{Z})$, suppose not.

Choose $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \setminus H$, s.t. $|a| + |c|$ is minimal.

(cont of $PSL_2(\mathbb{Z}) \simeq \mathbb{Z}_2 * \mathbb{Z}_3$)

Note that $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $BA = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. So $(AB)^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$, $(BA)^r = \begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix}$

(Assume first that $a \neq 0$, $c \neq 0$)

If $|a| \geq |c|$, we can choose r s.t. $|a + rc| < |a|$. Then,

$(AB)^r X = \begin{pmatrix} a+rc & b+rd \\ c & d \end{pmatrix}$, and $|a+rc| + |c| < |a| + |c| \Rightarrow !!$ $\left(\Rightarrow (AB)^r X \in H \Rightarrow X \in H \Rightarrow !! \right)$

If $|a| < |c|$, then choose s s.t. $|sa + c| < |c|$. Then,

$(BA)^{-s} X = \begin{pmatrix} a & b \\ sc+a & sb+d \end{pmatrix} \Rightarrow !!$

Hence $a = 0$ or $c = 0$. ($a = c = 0$ cannot occur, because $\det X = 1$!).

If $a = 0$, then $X = \begin{pmatrix} 0 & 1 \\ -1 & d \end{pmatrix}$ or $X = \begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}$, in which cases we have:

$X = BA^2 (AB)^{-d-1}$, or $X = B(AB)^{-d-1}$ $\Rightarrow X \in H \Rightarrow !!$

If $a \neq 0$, and $c = 0$: then $X = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}$ and we get that both of them is in $H \Rightarrow !!$ $\left(X = (AB)^b, \; X = A^2 (AB)^b \right)$.

So $SL_2(\mathbb{Z}) = \langle A, B \rangle$.

Define $A \mapsto \bar{A}$, $B \mapsto \bar{B}$ under the canonical mapping $SL_2(\mathbb{Z}) \longrightarrow \dfrac{SL_2(\mathbb{Z})}{(\pm I)} = PSL_2(\mathbb{Z})$

Note that $A^2 = -1 = B^3$, so $|\bar{A}| = 2$, $|\bar{B}| = 3$, and $PSL_2(\mathbb{Z}) = \langle \bar{A}, \bar{B} \rangle$.

By the mapping property of the coproduct, we get a surjective homomorphism

~~$\theta : \langle \bar{A} \rangle * \langle \bar{B} \rangle \longrightarrow$~~ $\theta : \langle a \rangle * \langle b \rangle \longrightarrow PSL_2(\mathbb{Z})$ have orders $\begin{cases} \langle a \rangle = 2 \\ \langle b \rangle = 3 \end{cases}$.
(with $a\theta = \bar{A}$, $b\theta = \bar{B}$).

Suppose $1 \neq x \in \ker\theta$. Since $a^2 = b^3 = 1$, x is a product of ab's and ab^2's, with perhaps a b or b^2 on the left, or an a on the right.

We can assume not both happen, because we could conjugate it to get another element in $\ker\theta$.

Then, would have $\overbrace{(B \text{ or } B^2) \cdot (AB)^r (AB^2)^s \cdots\cdots}^{C} (A) = \pm I$, $r, s \geq 0$

But $(AB)^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$, $(AB^2)^s = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}$. Then C has all nonnegative entries, and (with some positive entry) $C \neq \pm A$, or $\pm B$, $\pm B^2$ or $\pm I$ $\Rightarrow$ injective //

Exercise: Show that $SL_2(\mathbb{Z}) = \langle x, y \mid x^2 = y^3, x^4 = 1 \rangle$

Properties of free products

Theorem: Let $G = \underset{\lambda\in\Lambda}{\mathrm{Fr}}\, G_\lambda$

(i) Let $g \in G$ have ~~the~~ normal form $g = g_1 \cdots g_n$, $\underline{n > 1}$, and with $g_1 \neq g_n^{-1}$. Then g has infinite order.

(ii) If $g \in G$ has finite order, then some conjugate of g belongs to one of the G_λ's.

pf (i) We can assume that g_1 and g_n belong to different G_λ's

(otherwise, can form the conjugate $g_n g g_n^{-1}$ (has length still >1)) ← if $n=2$, then g_1 and g_2 cannot belong to the same G_λ, either!

m

Then, $g^m = g_1 \cdots g_n g_1 \cdots g_n \cdots g_1 \cdots g_n$ is in normal form ⇒ infinite order //

(ii) Suppose that the order of g is finite. Write $g = g_1 \cdots g_n$ in normal form

If g_1 and g_n belong to the same G_λ, then replace g by $g_n g g_n^{-1}$, which doesn't change its order.

So assume g_1 and g_n don't belong to the same G_λ.

Then $g^m = - - - -$ → can never be 1 ! ⇒ !! //

Corollary: If each G_λ is torsion-free, then $\underset{\lambda\in\Lambda}{\mathrm{Fr}}\, G_\lambda$ is torsion-free.

The Kuroš Subgroup Theorem

Let H be a subgroup of a free product $\underset{\lambda\in\Lambda}{\mathrm{Fr}}\, G_\lambda$. Then:

$$H = H_0 * \underset{\lambda, d_\lambda}{\mathrm{Fr}} \left(H \cap G_\lambda^{d_\lambda^{-1}} \right)$$

where
- H_0 is a free group
- d_λ belong to a set of (H, G_λ) double coset representatives.

(i.e. $G = \bigcup_{\lambda, d_\lambda} H d_\lambda G_\lambda$).

and $\lambda \in \Lambda$, and d_λ runs over all the double cosets representatives of (H, G_λ).

(cont statement of Kuroš sgp thm).

Furthermore, suppose that $|G:H| = m < \infty$. Then, the rank of the free group H_0 is
$$\sum_{\lambda\in\Lambda} (m - m_\lambda) + 1 - m$$
where m_λ is the number of (H, G_λ) double cosets in G.

Examples

1. If $G_\lambda \simeq \mathbb{Z}$, then this reduces to Nielsen-Schreier.
2. Suppose that each G_λ is abelian, then H is also a free product of abelian groups (hence this is a subgroup-closed class).
3. What are the finite subgroups of $PSL_2(\mathbb{Z})$?

   $PSL_2(\mathbb{Z}) \simeq \mathbb{Z}_2 * \mathbb{Z}_3$. Let $H \leq PSL_2(\mathbb{Z})$, with H finite.

   Then $H_0 = \{1\}$ (because H is finite!).

   Reading the theorem, then $H \simeq 1, \mathbb{Z}_2, \mathbb{Z}_3$.

[Can find the proof of the Thm in D. Robinson's book].

Generalized Free Products.

Consider a family of groups $\{G_\lambda, \lambda\in\Lambda\}$, and let $\varphi_\lambda : H \to G_\lambda$, where H is some group, and assume φ_λ are all injective.

So $H \simeq \operatorname{Im}(\varphi_\lambda) \leq G_\lambda$.

Def: The generalized free product or free product with amalgamated subgroup H determined by the previous data is defined to be $G := F/N$

where $F = \underset{\lambda\in\Lambda}{\operatorname{Fr}} G_\lambda$ and $N = \left\langle (h\varphi_\lambda)^{-1}(h\varphi_\mu) : \begin{matrix} h \in H \\ \lambda,\mu \in \Lambda \end{matrix} \right\rangle^F \leftarrow$ normal closure in F.

~~So~~ So $h^{\varphi_\lambda}N = h^{\varphi_\mu}N$ in G

$\therefore$ all the $H^{\varphi_\lambda}N/N$ are identified.

The simplest case is $\Lambda = \{1,2\}$, so $F = G_1 * G_2$, and will write

$G = G_1 \underset{H}{*} G_2$ (we ommit the maps $\varphi_1 : H \to G_1$, $\varphi_2 : H \to G_2$).

Or we can think of $H \leq G_1$, and $\varphi : H \to G_2$, and write $G_1 \underset{\varphi,H}{*} G_2$.

Example:

Consider $G = SL_2(\mathbb{Z})$. We saw that $G = \langle A, B \rangle$, where $A^2 = -I = B^3$,

So $|A| = 4$, $|B| = 6$.

We can see $G = \overset{\langle a \rangle}{\mathbb{Z}/4} * \overset{\langle b \rangle}{\mathbb{Z}/6} \Big/ \langle a^{-2}b^3 \rangle^F$

Write from now on $A^2 = B^3 = C$ (i.e. $C = -I$). $(C^2 = 1)$

We look for a "normal form" in G.

Note that, as $C \in Z(G)$ (it's a power of each generator), then we can write any element of G in the form

$$C^i A^{j_1} B^{k_1} A^{j_2} B^{k_2} \cdots A^{j_r} B^{k_r} \quad \text{where} \begin{cases} i \in \{0,1\} \\ j_t \in \{0,1\} \\ k_s \in \{0,1,2\} \end{cases}$$

This is unique, up to trivial factors, since $G/\langle C \rangle \cong PSL_2(\mathbb{Z}) \cong \langle \bar{A} \rangle * \langle \bar{B} \rangle$.

This is an instance of a normal form for $G_1 \underset{H}{*} G_2$.

Normal Form in a Generalized Free Product.

Given groups G_λ $(\lambda \in \Lambda)$, H, and injective homs $\varphi_\lambda : H \to G_\lambda$.

Write $F = \underset{\lambda \in \Lambda}{\mathrm{Fr}}\, G_\lambda$, $G = F/N$ (generalized free product), $N = \langle (h^{\varphi_\lambda})^{-1} h^{\varphi_\mu} \mid_{\lambda \in \Lambda, \mu \in \Lambda}^{h \in H} \rangle^F$.

For each $\lambda \in \Lambda$, choose a right transversal to $H^{\varphi_\lambda} (\leq G_\lambda)$ in G_λ.

Let the coset rep. of $H^{\varphi_\lambda} g_\lambda$ be called $\bar{g}_\lambda$, with H^{φ_λ} having representative 1_{G_λ}.

Take now any $f \in F$. Then $f = u_1 u_2 \cdots u_r$, in normal form in F,

so $u_i \in G_{\lambda_i}$, and $\lambda_i \neq \lambda_{i+1}$, $u_i \neq 1_{G_{\lambda_i}}$.

Define a sequence of elements $g_1, \dots, g_r$, where $g_i \in G_{\lambda_i}$ by:

Start with $g_r := u_r$. Then, write $g_r = h_r^{\varphi_{\lambda_r}} \overline{g_r}$ $(h_r \in H)$.

Then $f = u_1 \cdots u_{r-1} h_r^{\varphi_r} \overline{g_r}$. Write from now on $\varphi_i := \varphi_{\lambda_i}$.

~~As~~ Then $h_r^{\varphi_r} \equiv h_r^{\varphi_{r-1}} \pmod N$.

So $f \equiv u_1 u_2 \cdots \underbrace{(u_{r-1} h_r^{\varphi_{r-1}})}_{\uparrow G_{\lambda_{r-1}}} \overline{g}_r \pmod N$.

As $u_{r-1} h_r^{\varphi_{r-1}} \in G_{\lambda_{r-1}}$, we can write $u_{r-1} h_r^{\varphi_{r-1}} = h_{r-1}^{\varphi_{r-1}} \overline{g_{r-1}}$ where $\begin{cases} g_{r-1} = u_{r-1} h_r^{\varphi_{r-1}} \\ h_{r-1} \in H \end{cases}$

$\therefore f \equiv u_1 \cdots u_{r-2} (h_{r-1}^{\varphi_{r-1}} \overline{g_{r-1}}) \overline{g}_r \pmod N$.

$\equiv u_1 \cdots (u_{r-2} h_{r-1}^{\varphi_{r-2}}) \overline{g_{r-1}}\, \overline{g}_r \pmod N$ ...

Eventually, we get $f \equiv h^{\varphi_1} \overline{g}_1 \cdots \overline{g}_r \pmod N$

where each of the $\overline{g}_i$ are transversal elements, which can be assumed to be $\neq 1$

and $h^{\varphi_1} \in H^{\varphi_{\lambda_1}}$.

Def A <u>normal</u> ~~format~~ <u>form</u> of the element $f \in F$ wrt $\{\varphi_\lambda : H \to G_\lambda \mid \lambda \in \Lambda\}$ and right transversals to H^{φ_λ} in G_λ, is a formal expression:

$$h \overline{g}_1 \cdots \overline{g}_r \quad \text{where} \begin{cases} h \in H \\ g_i \in G_{\lambda_i},\ \overline{g}_i \text{ coset rep. of } H^{\varphi_{\lambda_i}} g_i . \end{cases}$$

and $\lambda_i \neq \lambda_{i+1}$, $\overline{g}_i \neq 1$,

Such that $f \equiv h^{\varphi_1} \overline{g}_1 \cdots \overline{g}_r \pmod N$.

We've just proven that normal forms exist. We need a uniqueness theorem, though.

Theorem: For each element f in $F = \underset{\lambda}{Fr}\, G_\lambda$ has a unique normal form wrt the injective homs $\varphi_\lambda : H \to G_\lambda$ and transversals to H^{φ_λ} in G_λ.

Pf/ we just need to prove uniqueness.
Just sketch (similar to the other two instances — free product, generalized free prod —).
Construct a permutation representation of $F/N = G$, on the set of all normal forms of elements of F.

Corollary: There are subgroups $\overline{H}$, $\overline{G_\lambda}$ of the generalized free product G such that:

i) $\overline{H} \cong H$

ii) $\overline{G_\lambda} \simeq G_\lambda$

iii) $G = \langle \overline{G_\lambda} \mid \lambda \in \Lambda \rangle$

iv) $\overline{G_\lambda} \cap \langle \overline{G_\mu} \mid \mu \neq \lambda \rangle = \overline{H}$.

Pf/ Define $\overline{H} = H^{\varphi_\lambda} N/N$ (indep of λ because of N).

$\overline{G_\lambda} = G_\lambda N/N$

Note that $\overline{H} \cong H$, since $H^{\varphi_\lambda} \cap N = 1$. (by uniqueness of the normal form).
For the same reason, $\overline{G_\lambda} \simeq G_\lambda$.
The rest is easy.

Notation:
We identify from now on h with $h^{\varphi_\lambda} N/N$, and g_λ with $g_\lambda N/N$, so $\overline{H} = H$, $\overline{G_\lambda} = G_\lambda$.
If $f \in F$, then we can identify fN with the normal form for f.

Theorem:

Let G be the generalized free product of $\{G_\lambda\}$, with amalgamating inj. homs. $\varphi_\lambda : H \to G_\lambda$.

i) If $g \in G$ has the normal form $g = h\bar{g}_1 \cdots \bar{g}_r$ ($\bar{g}_i$ coset rep. of H in G_λ), and if $\bar{g}_1, \bar{g}_r$ belong to different G_λ's, $(\neq 1)$ $(\neq 1)$ then g has infinite order.

ii) If $\exists \lambda_1 \neq \lambda_2 \in \Lambda$ s.t. $G_{\lambda_1} \neq H$, $G_{\lambda_2} \neq H$, then G contains an element of infinite order.

iii) An element of G which has finite order is the conjugate of an element of some G_λ.

Pf (ii) & (iii) follow clearly from (i).

(i) $g = h\bar{g}_1 \cdots \bar{g}_r$, ~~gd~~ $g_i \in G_{\lambda_i}$, $\lambda_1 \neq \lambda_r$.

Then $g^2 = h\bar{g}_1 \cdots \bar{g}_r h \bar{g}_1 \cdots \bar{g}_r$

Note that $\overline{g_r} h \in G_{\lambda_r}$, as $H \leqslant G_{\lambda_r}$. Write $\bar{g}_r h = h' \bar{g}_r'$. $\{ g_r' \in G_{\lambda_r}, h' \in H$

So $g^2 = h\bar{g}_1 \cdots \bar{g}_{r-1} h' \bar{g}_r' \bar{g}_1 \cdots \bar{g}_r \neq 1$, and in similar way, $g^m \neq 1$ $\forall m \geqslant 1$.

Corollary: Any generalized free product of torsion-free groups is torsion-free.

Example:

$F = \langle x \rangle * \langle y \rangle$, $|x| = 4$, $|y| = 6$. Then form $SL_2(\mathbb{Z}) = \langle x \rangle \underset{x^2=y^3}{*} \langle y \rangle$

So $\Lambda = \{1, 2\}$, $H = \langle h \rangle$, $|h| = 2$. $\varphi_1 : H \to \langle x \rangle$, $h \mapsto x^2$ $\quad \varphi_2 : H \to \langle y \rangle$, $h \mapsto x^3$

We have to choose transversals:

- To $\langle x^2 \rangle$ in $\langle x \rangle$: $\{1, x\}$
- To $\langle y^3 \rangle$ in $\langle y \rangle$: $\{1, y, y^2\}$

For example, will write $g = xyx^3y^2$ in normal form.

$$g = xy(x^3)y^2 = xy(x^2\underset{\uparrow}{x})\underset{\uparrow}{y^2} = x(yx^2)\underset{\uparrow}{x}\underset{\uparrow}{y^2} = x(yy^3)\underset{\uparrow}{x}\underset{\uparrow}{y^2} = x(y^3y)\underset{\uparrow}{x}\underset{\uparrow}{y^2} = (xy^3)\underset{\uparrow}{y}\underset{\uparrow}{x}\underset{\uparrow}{y^2} =$$

$$= (xx^2)\underset{\uparrow}{y}\underset{\uparrow}{x}\underset{\uparrow}{y^2} = \underset{\underset{H}{\Uparrow}}{(x^2)}\underset{\uparrow}{x}\underset{\uparrow}{y}\underset{\uparrow}{x}\underset{\uparrow}{y^2} \quad \text{(normal form)}.$$

HNN-extensions

Theorem: (G. Higman, B.H. Neumann, H. Neumann):
Let G be a group, with isomorphic subgroups H and K, $\theta : H \xrightarrow{\sim} K$.
Then, G can be embedded in a group $G^* = \langle t, G \rangle$, where
$h^t = h^\theta \quad \forall h \in H$. (So conjugation by t on H induces θ).

(we call G^* an HNN-extension of G.

Pf/ Let $\langle u \rangle$, $\langle v \rangle$ be infinite cyclic groups, and $\begin{cases} X := G * \langle u \rangle \\ Y := G * \langle v \rangle \end{cases}$.

Also, let $L = \langle G, H^u \rangle \leq X$

$M = \langle G, K^v \rangle \leq Y$

Notice that each element of L is uniquely expressible in the form:
$g_1 h_1^u g_2 h_2^u \cdots$ $\quad (g_i \in G, \ h_i \in H)$ (thanks to the normal form in X).

Hence $L = G * H^u$. Similarly, $M = G * K^v$

Define a homomorphism $\varphi : L \to M$ by $\begin{cases} g^\varphi = g \\ (h^u)^\varphi = (h^\theta)^v \end{cases}$

φ is an isomorphism because it has an inverse.

Next, form the generalized free product of X and Y with $L \overset{\varphi}{\simeq} M$ identified:

$$F := X \underset{L \overset{\varphi}{\simeq} M}{*} Y$$

Note that $G \leq F$ since $G \leq L \cap M$.

Let $h \in H$. Then, in F, $h^u = (h^u)^\varphi = (h^\theta)^v$. So $h^{uv^{-1}} = h^\theta$. Put $t = uv^{-1} \in F$.

Let $G^* = \langle t, G \rangle$, and note that this solves the problem.

//

Remark: If G is torsion-free, so is G^*.

Special case of HNN-exts: **Ascending** HNN-exts :

Let G be a group, and let θ be an injective endomorphism (not surjective to be interesting).

So $G \simeq G^{\theta} \leq G$. We can apply the HNN-theorem,

with $H = G$, $K = H^{\theta}$. We can form then the HNN-extn $G^* = \langle t, G \rangle$,

with $g^t = g^{\theta}$, $g \in G$.

As $G^t = G^{\theta} < G$, then get $G > G^t > G^{t^2} > \cdots$ and also, $G < G^{t^{-1}} < G^{t^{-2}} < \cdots$

Let $\bar{G} := \bigcup_{i=1,2,\ldots} G^{t^{-i}}$ and notice that $\bar{G} \triangleleft G^*$, and one can see that

$G^* = \langle t \rangle \ltimes \bar{G}$, $|t| = \infty$, $\langle t \rangle \cap \bar{G} = 1$.

Example: $G = \mathbb{Z}$, $\theta : g \mapsto \overset{g^2 \leftarrow \text{multiplicative notation}}{2g}$. The HNN-ext :

$G^* = \langle t, G \rangle = \langle t \rangle \ltimes \bar{G}$, $\bar{G} = \bigcup_{i \geq 1} G^{t^{-i}}$

Then $\bar{G} \simeq \{ \frac{m}{2^n} : m, n \in \mathbb{Z} \}$, by $\left(g^{t^{-n}}\right)^m \longmapsto \frac{m}{2^n}$.

Also, $G^* = \langle t, g \mid g^t = g^2 \rangle$ is f.presented metabelian ($\bar{G}$ abelian, $G^*/\bar{G}$ cyclic).

Embedding Theorems

Thm: Let G be a torsion-free group. Then, G can be embedded in a group $\bar{G}^*$ in which every pair of non-trivial elements is conjugate. ($\therefore$ class number $= 2$). Hence $\bar{G}^*$ is simple.

Comment: If G is a finite group with class number h, then $|G| \leq f(h)$ for some function f.
On the contrary, for infinite groups we see that having class number 2 doesn't tell much, because they could contain *any* torsion-free subgroup!

Pf of Thm

First, well-order the set $G \setminus 1 = \{x_\alpha \mid 1 \le \alpha < \beta\}$ where β is an ordinal number.
Put $G_1 = G$, and assume that we have constructed a chain of groups

G_γ, $\gamma < \alpha$ for some α, with $G_{\gamma_1} \le G_{\gamma_2}$ if $\gamma_1 \le \gamma_2$.

Such that for each $\gamma < \alpha$, all x_{γ_1} for $\gamma_1 < \gamma$ are conjugate in G_γ.

Show how to do it for α (transfinite induction):

- If α is a limit ordinal (has no predecessor).

  Define $G_\alpha := \bigcup_{\gamma < \alpha} G_\gamma$ and it clearly works: $\gamma_1, \gamma_2 < \alpha$, then $x_{\gamma_1}, x_{\gamma_2} \in G_\gamma$ for some $\gamma < \alpha$ $\Rightarrow$ conjugate in $G_\gamma \Rightarrow$ conj. in G_α.

- If α is <u>not</u> a limit ordinal, i.e. $\alpha - 1$ exists, and $G_{\alpha-1}$ has been constructed.

  Let $\gamma_1, \gamma_2 < \alpha$. So $\gamma_1, \gamma_2 \le \alpha - 1$. Can assume that $\gamma_2 = \alpha - 1$, and so consider $x_\gamma, x_{\alpha-1}$:

  Then $\langle x_\gamma \rangle \cong \langle x_{\alpha-1} \rangle$

  By the HNN-theorem, $\exists$ an HNN ext $G_\alpha = \langle t, G_{\alpha-1} \rangle$ s.t. $x_\gamma^t = x_{\alpha-1} \Rightarrow$ ✓.

So we've got a chain $\{G_\alpha\}$. Form the union $\bigcup G_\alpha =: G^*$.

Each pair of nontrivial elements of G are conjugated in G^*.

Finally, define another chain $G = G(0) \subseteq G(1) \subseteq \cdots$

by $G(n+1) := G(n)^*$ ← this previous construction.

and $\bar{G} := \bigcup_{n \ge 0} G(n)$. If $1 \ne x, y \in \bar{G}$, then $x, y \in G(n)$ for some n.

So x, y are conjugate in $G(n)^* = G(n+1) \Rightarrow$ conjugate in $\bar{G}$.

Theorem (by H.N.N also): Every countable group embeds in a two-generator group.

Pf/ Let $G = \{1 = g_0, g_1, g_2, \dots\}$ an enumeration.

Let F be free on $\{a, b\}$ (rk 2), and form $H := G * F$.

Define two subgroups of H:

- $A := \langle a, a^b, a^{b^2}, \cdots \rangle$
- $B := \langle bg_0, b^a g_1, b^{a^2} g_2, \cdots \rangle$

Clearly, each nontrivial word in $\{a, a^b, a^{b^2} \cdots\}$ cannot reduce to 1, because there will always be some b's in between. So A is a free group on $\{a, a^b, a^{b^2}, \cdots\}$.

Similarly, B is also free on $\{bg_0, b^a g_1, \cdots\}$ (even easier argument)

As the rank of both A and B is $\aleph_0$, there is an isomorphism

$$\varphi : A \to B \text{ by } (a^{b^i})^\varphi := b^{a^i} g_i .$$

Form HNN-extension $G^* = \langle t, H \rangle$ where conjugation by t in A induces the map φ.

Thus, $(a^{b^i})^t = (a^{b^i})^\varphi = b^{a^i} g_i$.

Consider the sgp $X := \langle a, t \rangle \leq G^*$.

Certainly, $X \ni a^t = a^\varphi = bg_0 = b$ as $g_0 = 1$. $\Rightarrow b \in X$.

So $(a^{b^i})^t \in X$, $(a^{b^i})^t = b^{a^i} g_i \in X \Rightarrow g_i \in X \ \forall i$.

$\therefore G \leq X$.

We end the course with some related embedding problems:

$\boxed{1}$ Let $\underline{\underline{V}}$ be a variety of groups, and let G be a countable group in $\underline{\underline{V}}$. Then G can be embedded in a 2-~~generator~~ generator group in the variety consisting of $\underline{\underline{V}}$-by-metabelian groups ($\exists N \triangleleft \bar{G}$ with $N \in \underline{\underline{V}}$, $\bar{G}/N$ metabelian)

↪ (taking $\underline{\underline{V}}$ to be the variety of all groups, we get the previous theorem).

↪ taking $\underline{\underline{V}}$ ~~to~~ to be the variety of abelian groups, then every countable abelian group embeds in a two generator soluble group, of derived length ≤ 3.

$\boxed{2}$ <u>Thm</u> (The Higman Embedding Thm):

A finitely-generated group G can be embedded in a finitely-presented one if, and only if, G has a recursive presentation.

(i.e. the defining relations form a recursively enumerable set).

Pf

$\Rightarrow$) easy.

$\Leftarrow$) very hard.