

Infinite Groups

Notes from the lectures of Prof. Lorensen
TU Vienna, Winter 2007¹

Clemens Koppensteiner

July 29, 2009

Contents

1 Prerequisites	2
1.1 Notation and Basic Definitions	2
1.2 Isomorphism Theorems	3
1.3 Sylow Groups	3
1.4 Finitely Generated Abelian Groups	4
1.5 Miscellaneous Theorems	4
1.6 Semidirect Products	4
1.7 Tensor Product	5
2 Subgroups of Finite index	5
3 Solvable Groups	7
4 Nilpotent Groups	9
5 Polycyclic Groups	16
6 Free Groups	18
7 Residual Finiteness	20
7.1 Residual p -Groups	22
8 HNN Extensions	24

¹These notes have *not* been reviewed by Prof. Lorensen

1 Prerequisites

1.1 Notation and Basic Definitions

Throughout this document G is a group. The symbol 1 is used both for the identity element in G and the trivial subgroup. Sometimes the name of the group is added as a subscript, i.e. 1_G . For abelian groups, 0 may be used instead of 1 .

The word “map” will always mean a homomorphism. The notation $H \xrightarrow{\phi} G$ is used to denote that ϕ is an injective map from H to G . Similarly $H \xrightarrow{\phi} G$ means that ϕ is a surjective map.

The symbols $H \leq G$ and $H \triangleleft G$ will denote that H is a subgroup resp. normal subgroup of G .

Definition 1.1. Let G be a group and $x, y \in G$. We define

$$y \cdot x := yxy^{-1}$$

and

$$[x, y] := xyx^{-1}y^{-1} = (x \cdot y)y^{-1}.$$

$[x, y]$ is called the *commutator* of x and y . Inductively

$$[x_1, x_2, \dots, x_n] := [x_1, [x_2, \dots, x_n]]$$

is called the *commutator of weight n* .

Remark 1.2. This is not the most common definition of the commutator. Most group theorists define it as $x^{-1}y^{-1}xy$. However the present definition will be more useful in this lecture.

Proposition 1.3.

1. $[x, y]^{-1} = [y, x]$
2. $[xy, z] = (x \cdot [y, z])[x, z]$
3. $[x, yz] = [x, y](y \cdot [x, z])$
4. (*Hall-Witt formula*) $(y \cdot [x, y^{-1}, z])(z \cdot [y, z^{-1}, x])(x \cdot [z, x^{-1}, y]) = 1$

Definition 1.4. Let G be a group. For $a \in G$

$$C_G(a) := \{g \in G : ag = ga\}$$

is called the *centralizer* of a in G . For any subset S of G the centralizer of S in G is

$$C_G(S) := \{g \in G : gs = sg \forall s \in S\}.$$

$Z(G) := C_G(G) = \{g \in G : ga = ag \forall a \in G\}$ is called the *center* of G .

$C_G(S)$ is a subgroup of G . The centralizer of a normal subgroup is again normal. The center is a normal subgroup and is abelian. It is also characterized by $Z(G) = \{g \in G : [g, a] = 1 \forall a \in G\}$.

Definition 1.5. Let G be a group and S a subset of G . Then the *normalizer* of S in G is

$$N_G(S) := \{g \in G : gS = Sg\}.$$

The normalizer is always a subgroup of G . If S is a subgroup of G , then $N_G(S)$ is the largest subgroup H of G such that $S \triangleleft H$.

Definition 1.6. Two elements $a, b \in G$ are called *conjugate* if there exists an element $g \in G$ with $gag^{-1} = b$. Conjugacy is an equivalence relation and the equivalence classes are called *conjugacy classes*.

Proposition 1.7 (Class Formula; Class Equation). *Let C be set of representatives for the distinct conjugacy classes of G . Then*

$$|G| = \sum_{x \in C} [G : C_G(x)].$$

If C' is a set of representatives for the conjugacy classes with more than one element, then

$$|G| = |Z(G)| + \sum_{x \in C'} [G : C_G(x)].$$

1.2 Isomorphism Theorems

Theorem 1.8. *Let G be a group and K, H two normal subgroups with $K \subseteq H$. Then K is normal in H and*

$$(G/K)/(H/K) \cong G/H.$$

Theorem 1.9. *Let G be a group and H, K two subgroups with $H \subseteq N_G(K)$. Then*

$$H/(H \cap K) \cong HK/K.$$

1.3 Sylow Groups

Let G be a finite group and let p be a prime number dividing the order of G .

Definition 1.10. Let $H \leq G$ be of order p^α (then $p^\alpha \mid |G|$). Then H is called a *p-subgroup* of G . If $p^{\alpha+1} \nmid |G|$, H is called a *Sylow p-subgroup*.

Theorem 1.11 (Sylow's theorems). *Let p be a prime number dividing $|G|$. Then the following statements hold:*

1. G has a Sylow p -subgroup.
2. All Sylow p -subgroups of G are conjugate.
3. The number of Sylow p -subgroups of G is a divisor of $|G|$ congruent to 1 mod p .

1.4 Finitely Generated Abelian Groups

Theorem 1.12. *Let G be a finitely generated abelian group. Then G is isomorphic to*

$$\mathbb{Z}^n \oplus \mathbb{Z}/p_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_m\mathbb{Z}$$

where $n \geq 0$ and p_1, \dots, p_m are (not necessarily distinct) powers of prime numbers. In particular, G is finite if and only if $n = 0$. The values of n and p_1, \dots, p_m are (up to order) uniquely determined by G .

Thus G is isomorphic to a direct sum of a free abelian group and a finite abelian group, the *torsion subgroup* of G .

Definition 1.13. A group that contains no elements of finite order is called *torsion-free*.

1.5 Miscellaneous Theorems

Theorem 1.14 (Correspondence Theorem). *Let N be a normal subgroup of G , \mathcal{S} the set of all subgroups of G containing N and \mathcal{T} the set of all subgroups of G/N . Then the map $H \mapsto H/N$ is a bijection between \mathcal{S} and \mathcal{T} that preserves normality and indices.*

Theorem 1.15. *If $M, N \triangleleft G$, $G = MN$ and $M \cap N = 1$, then $G \cong M \times N$.*

1.6 Semidirect Products

Definition 1.16. Let N be a group. Then a homomorphism $\omega: G \rightarrow \text{Aut}(N)$ is called an *action of G on N* . For $g \in G$, $a \in N$ we write $g \cdot a$ for $\omega(g)(a)$. N is called a (*left*) G -*group* and we say that G acts on N by ω .

Example 1.1. Let $N \triangleleft G$. Then G acts on N by conjugation: $g \cdot a = gag^{-1}$.

Definition 1.17. Assume G acts on N by $\omega: G \rightarrow \text{Aut}(N)$. Then the *semidirect product of N with G with respect to ω* is the set $N \times G$ together with the operation

$$(a, g)(a', g') := (a(g \cdot a'), gg')$$

and is denoted by $N \rtimes_{\omega} G$.

G is a subgroup and N a normal subgroup of $N \rtimes_{\omega} G$.

If $N \triangleleft G$, $H \leq G$ and $\omega: H \rightarrow \text{Aut}(N)$ arises from conjugation, the semidirect product is simply written as $N \rtimes H$.

Theorem 1.18. *If $N \triangleleft G$, $H \leq G$, $G = NH$ and $N \cap H = 1$, then $G \cong N \rtimes H$.*

Examples 1.2.

1. The dihedral group of order $2n$ can be decomposed into $D_n = C_n \rtimes C_2$ where C_n are the rotations and C_2 is one reflection.
2. Similarly $S_n = A_n \rtimes C_2$.

3. Let $N = \bigoplus_{i=-\infty}^{\infty} \mathbb{Z}$ and $G = \mathbb{Z}$. G acts on N by $1 \cdot (x_i)_{i=-\infty}^{\infty} := (x_{i-1})_{i=-\infty}^{\infty}$ (right shift). $\Gamma := N \rtimes_{\omega} G$.

Let $t = ((0), 1)$ and $x = ((\delta_{i0})_{i=-\infty}^{\infty}, 0)$. Then Γ is generated by x and t ($t^k x t^{-k} = ((\delta_{ik})_{i=-\infty}^{\infty}, 0)$), but it has a subgroup $\langle N \rangle$, which is not finitely generated.

1.7 Tensor Product

Definition 1.19. Let A and B be abelian groups. Then their *tensor product* $A \otimes B$ is the abelian group generated by all $a \otimes b$, $a \in A$, $b \in B$ subject to the relations

$$(a + a') \otimes b = a \otimes b + a' \otimes b,$$

$$a \otimes (b + b') = a \otimes b + a \otimes b'.$$

2 Subgroups of Finite index

Notation: The symbols $H \leq_f G$ and $H \triangleleft_f G$ denote that H is a (normal) subgroup of finite index in G .

In example 1.2.3 we saw that a subgroup H of a finitely generated group G does not need to be finitely generated. The following theorem states one sufficient condition for H to be finitely generated.

Theorem 2.1. *If G is finitely generated and $H \leq G$ with $[G : H] \leq \infty$, then H is finitely generated*

Proof. Let $G = \langle g_1, \dots, g_n \rangle$ and $g_{n+1} = g_1^{-1}, \dots, g_{2n} = g_n^{-1}$, so that G is generated by positive powers of g_1, \dots, g_{2n} . Let $m = [G : H]$ and Hx_1, \dots, Hx_m be a complete list of right cosets with $x_1 = 1$. For each x_i and g_j their product is in some coset $Hx_{f(i,j)}$. So there exists $h_{ij} \in H$ with $x_i g_j = h_{ij} x_{f(i,j)}$ ($i = 1, \dots, m$, $j = 1, \dots, 2n$). We claim that $\{h_{ij}\}$ generate H .

To see this let h be an arbitrary element of H . Then $h = g_{j_1} g_{j_2} \cdots g_{j_r} = x_1 g_{j_1} g_{j_2} \cdots g_{j_r} = h_{1g_{j_1}} x_{f(1,j_1)} g_{j_1} g_{j_2} g_{j_3} \cdots g_{j_r} = \cdots = h_{p_1 q_1} h_{p_2 q_2} \cdots h_{p_r q_r} x_u$. Because h and all $h_{p_i q_i}$ are in H , x_u must lie in H and therefore $x_u = 1$. \square

Let $H \leq G$ be any subgroup and $X = \{aH : a \in G\}$ be the set of left cosets of H . Then G acts on X by $g \cdot aH = gaH$. This induces a homomorphism $\phi : G \rightarrow S(X)$ (where $S(X)$ are the permutations of X) such that $\phi(g)$ is the permutation $aH \mapsto gaH$. We can observe the following properties of $\ker \phi$:

1. $\ker \phi \leq H$ ($x \in \ker \phi \Rightarrow xH = H \Rightarrow x \in H$)
2. $\ker \phi = \bigcap_{g \in G} gHg^{-1}$ ($x \in \ker \phi \Leftrightarrow xaH = aH \Leftrightarrow a^{-1}xaH = H \Leftrightarrow a^{-1}xa \in H \Leftrightarrow x \in aHa^{-1} \forall a \in G$)
3. $\ker \phi$ is the largest normal subgroup of G contained in H . In other words: $N \triangleleft G$, $N \leq H \Rightarrow N \leq \ker \phi$.

Definition 2.2. For the map ϕ defined above, the kernel $\ker \phi$ is called the *normal core* of H and is denoted by $\text{core } H$.

If H is of finite index, i.e. $[G : H] = |X| = n < \infty$, then $S(X) = S_n$ is finite and by the homomorphism theorem $[G : \ker \phi] \leq n! < \infty$. This proves the following theorem:

Theorem 2.3. *Any subgroup of finite index contains a normal subgroup of finite index.*

Theorem 2.4. *If G is finitely generated and $n \in \mathbb{Z}_{>0}$, then G contains only finitely many subgroups of index n .*

Proof. If G is finitely generated, then there are only finitely many possibilities for $\phi : G \rightarrow S_n$ and so there are only finitely many possible kernels of such maps ϕ . Thus there are only finitely many possibilities for H . \square

Definition 2.5. $N \leq G$ is called a *characteristic subgroup* if for all $\alpha \in \text{Aut}(G)$ $\alpha(N) = N$. To denote that N is a characteristic subgroup of G , we will use the symbol $N \triangleleft_{\text{char}} G$.

Remark 2.6. Every characteristic subgroup is normal.

Lemma 2.7. *Let N be a subgroup of G . If $\alpha(N) \subseteq N$ for every $\alpha \in \text{Aut}(G)$, then N is already characteristic.*

Proof. For every α the inverse α^{-1} is also an automorphism, so $\alpha^{-1}(N) \subseteq N$ and therefore $N = \alpha(\alpha^{-1}(N)) \subseteq \alpha(N)$. \square

Theorem 2.8. *If $[G : H] < \infty$ and G is finitely generated, then H contains a characteristic subgroup N of G such that $[G : N] < \infty$*

Proof. Let $N = \bigcap_{\alpha \in \text{Aut}(G)} \alpha(H)$. Then for each $\beta \in \text{Aut}(G)$

$$\beta(N) = \bigcap_{\alpha \in \text{Aut}(G)} \beta\alpha(N) = N$$

and therefore N is characteristic. We have to show that it is of finite index.

For every $\alpha \in \text{Aut}(G)$ the index of $\alpha(H)$ in G is equal to $[G : H]$ and by theorem 2.4 there are only finitely many subgroups of the form $\alpha(H)$. Let $\alpha_1(H), \dots, \alpha_r(H)$ be all of them. Then $N = \bigcap_{i=1}^r \alpha_i(H)$ is a finite intersection of subgroups of finite index. Thus N is of finite index. \square

Proposition 2.9. *Let G be finitely generated, $\phi : G \rightarrow G$ a homomorphism and $N \triangleleft G$ with $[G : N] < \infty$. Then N contains a subgroup $M \triangleleft G$ such that $[G : M] < \infty$ and $\phi(M) \subseteq M$.*

The proof of this proposition is left as an exercise.

3 Solvable Groups

We will study three generalizations of abelian groups: solvable groups, polycyclic groups and nilpotent groups. For this we need the following definition.

Definition 3.1. A series of the form

$$1 = N_0 \triangleleft N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_{r-1} \triangleleft N_r = G$$

is called a *normal series of length r* .

If Σ and Δ are two normal series with $\Sigma \subseteq \Delta$, then Δ is called a *refinement* of Σ .

Two normal series

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = G$$

$$1 = M_0 \triangleleft M_1 \triangleleft \cdots \triangleleft M_s = G$$

are called isomorphic, if $r = s$ and $N_i/N_{i-1} \cong M_i/M_{i-1}$ for $i = 1, \dots, r$.

Before we go on to define solvable groups, we will have a look at the following important theorem about normal series:

Theorem 3.2 (Schreier's Refinement Theorem). *Let*

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = G$$

$$1 = M_0 \triangleleft M_1 \triangleleft \cdots \triangleleft M_s = G$$

be two normal series. They possess isomorphic refinements.

To prove this we need the following lemma:

Lemma 3.3 (Zassenhaus). *Let A_1, A_2, B_1, B_2 be subgroups of G with $A_1 \triangleleft A_2$ and $B_1 \triangleleft B_2$ and let $D_{ij} = A_i \cap B_j$. Then*

1. $A_1 D_{21} \triangleleft A_1 D_{22}$ and $B_1 D_{12} \triangleleft B_1 D_{22}$;
2. $A_1 D_{22}/A_1 D_{21} \cong B_1 D_{22}/B_1 D_{12}$.

Proof. Because $D_{21} \triangleleft D_{22}$ and $D_{12} \triangleleft D_{22}$ the first statement is trivial.

We use the isomorphism theorem $NH/N \cong H/(N \cap H)$ with $N = A_1 D_{21}$ and $H = D_{22}$ to get $A_1 D_{22}/A_1 D_{21} \cong D_{22}/(A_1 D_{21} \cap D_{22}) = D_{22}/D_{12} D_{21}$. The last equality follows from $a_1 d_{21} = d_{22} \in A_1 D_{21} \cap D_{22} \Rightarrow a_1 = d_{22} d_{21}^{-1} \in B_2$, so $a_1 \in D_{12}$. The other direction is obvious. By a symmetric argument it follows that $B_1 D_{22}/B_1 D_{12} \cong D_{22}/D_{21} D_{12}$ and because D_{12} and D_{21} are normal in D_{22} they commute. \square

Proof of Schreier's theorem. Let $N_{ij} = N_i(N_{i+1} \cap M_j)$ and $M_{ij} = M_j(N_i \cap M_{j+1})$ for $0 \leq i \leq r$ and $0 \leq j \leq s$. These series are refinements of the original normal series with

$$N_i = N_{i0} \triangleleft N_{i1} \triangleleft \cdots \triangleleft N_{is} = N_{i+1},$$

$$M_j = M_{0j} \triangleleft M_{1j} \triangleleft \cdots \triangleleft N_{rj} = M_{j+1}.$$

We have to show that $N_{i(j+1)}/N_{ij} \cong M_{(i+1)j}/M_{ij}$. To do this we apply the lemma with $A_1 = N_i$, $A_2 = N_{i+1}$, $B_1 = M_j$ and $B_2 = M_{j+1}$. We have $A_1 D_{22}/A_1 D_{21} = N_i(N_{i+1} \cap M_{j+1})/N_i(N_{i+1} \cap M_j) = N_{i(j+1)}/N_{ij}$ and similarly $B_1 D_{22}/B_1 D_{12} = M_{(i+1)j}/M_{ij}$. \square

Definition 3.4. The subgroup generated by all commutators is called the *commutator subgroup* and is denoted by $G' := \langle [x, y] : x, y \in G \rangle$.

G' is a characteristic subgroup of G because $\alpha([x, y]) = [\alpha(x), \alpha(y)]$, $\alpha \in \text{Aut}(G)$. Obviously G/G' is abelian. Furthermore if $N \triangleleft G$ and G/N is abelian, then $G' \leq N$.

Definition 3.5. $G_{ab} := G/G'$ is called the *abelianization* of G .

Definition 3.6. $G^{(1)} = G'$ is also called the *first derived subgroup* of G . $G^{(2)} = G'' = (G')'$ is the *second derived subgroup* and in general $G^{(n)} = (G^{(n-1)})'$ is the *n-th derived subgroup*. The series

$$\cdots \leq G^{(3)} \leq G^{(2)} \leq G^{(1)} \leq G$$

is called the *derived series* of G .

For every n , $G^{(n)}$ is a characteristic subgroup of G , because from $H \triangleleft_{char} K$ and $K \triangleleft_{char} G$ follows $H \triangleleft_{char} G$ (note that this is not true for normality). The factor group $G_{ab}^{(n)} := G^{(n)}/G^{(n-1)}$ is always abelian.

Definition 3.7. A group G is called *solvable* if $G^{(n)} = 1$ for some n . The smallest n for which $G^{(n)} = 1$ is called the *derived length* of G .

Example 3.1. Simple non-abelian groups are never solvable.

A group with derived length 1 is always abelian. Groups with derived length 2 are called *metabelian*.

Proposition 3.8. G is solvable if and only if G has a normal series

$$1 = N_r \triangleleft N_{r-1} \triangleleft \cdots \triangleleft N_1 \triangleleft N_0 = G,$$

such that N_i/N_{i+1} is always abelian. Then the derived length of G is the length of the shortest such normal series.

Proof. $G' \leq N_1$ and by induction $G^{(i)} \leq N_i$. Therefore $G^{(r)} = 1$. \square

Definition 3.9. A sequence $N \xrightarrow{\iota} G \xrightarrow{\epsilon} Q$ is called *exact*, if $\iota(N) = \ker \epsilon$. Such a sequence is also called a *group extension*.

By identifying N with $\iota(N)$ in the exact sequence above we have $G/N \cong Q$. A group extension always corresponds to a normal series in G : $1 \triangleleft N \triangleleft G$.

Examples 3.2.

1. $C_3 \twoheadrightarrow S_3 \twoheadrightarrow C_2$ is a group extension and because C_2 is abelian, S_3 is solvable (and metabelian).

2. $C_2 \times C_2 \twoheadrightarrow A_4 \twoheadrightarrow C_3$ is a group extension with $C_2 \times C_2$ mapped to $\{(1), (12)(34), (13)(24), (14)(23)\}$ and therefore A_4 is solvable.
3. A_n is simple for $n \geq 5$, therefore it is not solvable and because subgroups of solvable groups are always solvable, S_n is not solvable for $n \geq 5$.
4. Let G be the group from example 1.2.3. Then $\bigoplus_{i=-\infty}^{\infty} \mathbb{Z} \twoheadrightarrow G \twoheadrightarrow \mathbb{Z}$ is a group extension and G is solvable.

Definition 3.10. A class \mathcal{C} of groups is said to be *closed under the formation of group extensions* if for every group extension $N \twoheadrightarrow G \twoheadrightarrow Q$ with $N, Q \in \mathcal{C}$, G is also in \mathcal{C} .

Theorem 3.11. *The class of solvable groups is the smallest class of groups that contains the abelian groups and is closed under forming extensions.*

4 Nilpotent Groups

For subgroups H, K of G define $[H, K] := \langle [h, k] : h \in H, k \in K \rangle$. If H and K are normal (characteristic) in G , then $[H, K]$ is normal (characteristic) in G .

Definition 4.1. Let $\gamma_1 G := G$, $\gamma_2 G := G'$ and inductively $\gamma_i G := [G, \gamma_{i-1} G]$. The series

$$\cdots \leq \gamma_4 G \leq \gamma_3 G \leq \gamma_2 G \leq \gamma_1 G = G$$

is called the *lower (or descending) central series* of G .

By induction, $\gamma_i G \triangleleft_{char} G$ for all $i \in \mathbb{N}^+$.

Definition 4.2. Define $Z_0(G) := 1$, $Z_1(G) := Z(G)$ and inductively $Z_i(G)$ by

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$$

or equivalently $Z_i(G) = \{x \in G : [x, g] \in Z_{i-1}(G) \forall g \in G\}$. The series

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq Z_3(G) \leq \dots$$

is called the *upper (or ascending) central series* of G .

Again $Z_i(G) \triangleleft_{char} G$ for all $i \in \mathbb{N}_0$.

Definition 4.3. A series

$$1 = G_0 \leq G_1 \leq G_2 \leq \dots \leq G_n = G$$

of normal subgroups G_i of a group G is called a *central series* if $G_i/G_{i-1} \leq Z(G/G_{i-1})$ or equivalently if $[G_i, G] \leq G_{i-1}$.

Theorem 4.4. *Let $1 = G_0 \leq G_1 \leq \dots \leq G_n = G$ be a central series. Then*

1. $G_i \leq Z_i(G)$ for $0 \leq i \leq n$;
2. $\gamma_i G \leq G_{n+1-i}$ for $1 \leq i \leq n+1$.

Proof. The proofs for both statements are by induction on n . For $i = 0$, $G_0 = 1 = Z_0(G)$. Assume $G_{i-1} \leq Z_{i-1}(G)$. Then $[G_i, G] \leq G_{i-1} \leq Z_{i-1}(G)$ and by the second definition of the upper central series $G_i \leq Z_i(G)$.

The second statement: For $i = 1$, $\gamma_1 G \leq G = G_n$. Now assume $\gamma_{i-1} G \leq G_{n-i+2}$. Then

$$\gamma_i G = [G, \gamma_{i-1} G] \leq [G, G_{n-i+2}] \leq G_{n-i+1}.$$

□

Corollary 4.5. $\gamma_{n+1} G = 1$ if and only if $Z_n(G) = G$.

Proof. First assume that $\gamma_{n+1} G = 1$ and apply the first statement of the theorem above to the last term of $1 = \gamma_{n+1} G \leq \gamma_n G \leq \cdots \leq \gamma_2 G \leq \gamma_1 G = G$ to get $G = \gamma_1 G \leq Z_n(G)$.

Similarly apply the second statement to $Z_0(G)$ in the ascending central series to get the reverse implication. □

Definition 4.6. If $\gamma_{n+1} G = 1$ for some n (or equivalently $Z_n(G) = G$), then G is called *nilpotent*. The smallest n such that $\gamma_{n+1} G = 1$ (i.e. the length of the shortest central series in G) is called the *nilpotency class* of G and one writes $n = \text{nil } G$.

Remark 4.7. Every group with nilpotency class 1 is abelian.

Remark 4.8. Every nilpotent group is solvable, but not every solvable group is nilpotent. For instance S_3 is solvable, but $Z(S_3) = 1$ and therefore S_3 cannot be nilpotent.

Definition 4.9. A group extension $N \hookrightarrow G \twoheadrightarrow Q$ is called a *central extension* if $N \leq Z(G)$.

Definition 4.10. A class \mathcal{C} of groups is said to be *closed under the formation of central extensions* if for every central extension $N \hookrightarrow G \twoheadrightarrow Q$ with $N, Q \in \mathcal{C}$, G is also in \mathcal{C} .

Theorem 4.11. *The class of nilpotent groups is the smallest class of groups that contains the abelian groups and is closed under forming central extensions.*

Lemma 4.12. *If $|G| = p^n$ for a prime number p and $n > 0$, then $Z(G) \neq 1$.*

Proof. Let a_1, \dots, a_k be a complete set of representatives of the conjugacy classes with cardinality greater than 1. Then by the class formula:

$$|G| = |Z(G)| + \sum_{i=1}^k [G : C_G(a_i)]$$

Since $p \mid |G|$ and by Lagrange's theorem $p \mid [G : C_G(a_i)]$ for $i = 1, \dots, k$, p must also divide $|Z(G)| \geq 1$. Thus $|Z(G)| \geq p > 1$. □

Theorem 4.13. *If $|G| = p^n$ for a prime number p , then G is nilpotent.*

Proof. Suppose G is not nilpotent. Then $Z_i(G) \neq G$ for all $i \in \mathbb{N}$. By the last theorem $Z(G) \neq 1$. Also $|G/Z_i(G)| = p^l > 1$ and therefore $Z(G/Z_i(G)) \neq 1$. Then the upper central series cannot become stationary:

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq Z_3(G) \leq \dots$$

This is a contradiction to the finite order of G . \square

In an abelian group every subgroup is normal. Clearly this statement does not hold for all nilpotent groups. It is however possible to obtain a weaker version of this statement.

Definition 4.14. A subgroup H of G is called *subnormal* if there exists a normal series

$$H = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_r = G.$$

Theorem 4.15. *If G is nilpotent, then every subgroup is subnormal.*

Proof. Let c be the nilpotency class of G and $H \leq G$. Then

$$H = HZ_0(G) \leq HZ_1(G) \leq HZ_2(G) \leq \dots \leq HZ_c(G) = G.$$

We will show that $HZ_{i-1}(G) \triangleleft HZ_i(G)$: For $z \in Z_i(G)$, $g \in G$

$$zgz^{-1} \equiv g \pmod{Z_{i-1}(G)}$$

and thus $zHZ_{i-1}(G)z^{-1} = HZ_{i-1}(G)$. For $h \in H$

$$hHZ_{i-1}(G)h^{-1} = hHh^{-1}hZ_{i-1}(G)h^{-1} = HZ_{i-1}(G),$$

because $Z_{i-1}(G) \triangleleft G$. \square

The following theorem is a partial classification of finite nilpotent groups:

Theorem 4.16. *If G is a finite nilpotent group, then G is a direct product of groups of prime power order.*

To proof this, we need a lemma:

Lemma 4.17. *If P is a subnormal Sylow subgroup of a group G , then P is normal in G .*

Proof. Let $P \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_r = G$. We will show by induction, that P is normal in H_i . Assume that $P \triangleleft H_{i-1}$. Then by Sylow's second theorem, P is the unique Sylow p -subgroup of H_{i-1} . For every $g \in H_i$, $gPg^{-1} \leq H_{i-1} \triangleleft H_i$ and gPg^{-1} is a Sylow p -subgroup (contained in H_{i-1}). Therefore $gPg^{-1} = P$ and $P \triangleleft H_i$. \square

Proof of Theorem 4.16. Every Sylow p -subgroup of G is normal in G by the lemma and theorem 4.15. Therefore it is the unique Sylow p -subgroup. Two Sylow subgroups for different prime numbers have trivial intersection, because their orders are relatively prime. Every element of G can be written as a product of elements of Sylow subgroups. Thus G is the direct product of its Sylow subgroups. \square

Examples 4.1.

- The group $G = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$ with the usual matrix multiplication is called the *Heisenberg group*.

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$$

$$\left[\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & ac' - a'c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$Z(G) = \begin{pmatrix} 1 & 0 & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

So $Z(G) = G'$ and $G/Z(G)$ is abelian. Therefore $Z_2(G) = G$ and the Heisenberg group is nilpotent of class 2.

- This can be generalized in the following way: Let R be any commutative ring with 1 and consider the *unidiagonal triangular matrices*

$$\mathcal{U} = \mathcal{U}(n, R) = \underbrace{\left. \begin{pmatrix} 1 & R & \dots & R \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & R \\ 0 & \dots & 0 & 1 \end{pmatrix} \right\}}_n n.$$

This is a group under matrix multiplication with the following upper central series:

$$Z(\mathcal{U}) = \begin{pmatrix} 1 & 0 & \dots & 0 & R \\ 0 & 1 & \ddots & & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

$$Z_2(\mathcal{U}) = \begin{pmatrix} 1 & 0 & \dots & 0 & R & R \\ 0 & 1 & \ddots & & 0 & R \\ \vdots & \ddots & \ddots & \ddots & & 0 \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

Proof. First define a surjective map

$$\lambda^n: \begin{cases} G_{ab} \otimes (\gamma_{n-1}G/\gamma_nG) \twoheadrightarrow \gamma_nG/\gamma_{n+1}G \\ \bar{x} \otimes \bar{y} \mapsto \overline{[x, y]} \end{cases}.$$

To show that λ^n is well-defined we need

$$[xy, z] \equiv [x, z][y, z] \pmod{\gamma_{n+1}G} \quad \text{for } x, y \in G, z \in \gamma_{n-1}G$$

and

$$[x, yz] \equiv [x, y][x, z] \pmod{\gamma_{n+1}G} \quad \text{for } x \in G, y, z \in \gamma_{n-1}G.$$

To show the first statement note that everything in γ_nG commutes with everything in G modulo $\gamma_{n+1}G$, so that 1.3 gives

$$[xy, z] = (x \cdot [y, z])[x, z] \equiv [y, z][x, z] \equiv [x, z][y, z] \pmod{\gamma_{n+1}G}.$$

The second statement can be shown in a similar way.

Now define χ^n by induction on n : $\chi^1 := \text{id}$. Assume that χ^{n-1} is defined, so that we have

$$\chi^{n-1}: \underbrace{G_{ab} \otimes \cdots \otimes G_{ab}}_{n-1} \twoheadrightarrow \gamma_{n-1}G/\gamma_nG,$$

$$\lambda^n: G_{ab} \otimes (\gamma_{n-1}G/\gamma_nG) \twoheadrightarrow \gamma_nG/\gamma_{n+1}G.$$

Define χ^n by the following composition:

$$\begin{aligned} \underbrace{G_{ab} \otimes \cdots \otimes G_{ab}}_n &\twoheadrightarrow G_{ab} \otimes \underbrace{(G_{ab} \otimes \cdots \otimes G_{ab})}_{n-1} \\ \text{id} \otimes \chi^{n-1} &\xrightarrow{\quad} G_{ab} \otimes (\gamma_{n-1}G/\gamma_nG) \xrightarrow{\lambda^n} \gamma_nG/\gamma_{n+1}G. \end{aligned}$$

This composition maps

$$\bar{x}_1 \otimes \cdots \otimes \bar{x}_n \mapsto \bar{x}_1 \otimes \overline{[x_2, \dots, x_n]} \mapsto \overline{[x_1, \dots, x_n]}.$$

□

Definition 4.21. A group-theoretic property \mathbb{P} is called *extendable* if the following statements hold:

1. Whenever A and B are abelian groups with property \mathbb{P} then $A \otimes B$ has \mathbb{P} .
2. Whenever A has \mathbb{P} and $\phi: A \twoheadrightarrow B$ is an epimorphism of abelian groups then B has \mathbb{P} .
3. Whenever $A \twoheadrightarrow G \twoheadrightarrow Q$ is a central extension where A and Q have \mathbb{P} then G has \mathbb{P} .

Examples 4.2. The following properties are all extendable:

- Being the trivial group.
- Being finite.

- Being finitely generated.
- Being a Π -group. (When Π is a set of primes, a Π -group is a group in which every element has finite order whose prime divisors are all elements of Π .)
- Being Π -divisible. (A group G is called Π -divisible if for every $g \in G$ and $p \in \Pi$ the equation $x^p = g$ has a solution.)

We can now formulate the influence of the structure of G_{ab} on G mentioned above:

Theorem 4.22. *Let \mathbb{P} be an extendable property and G a nilpotent group. If G_{ab} has \mathbb{P} , then G has \mathbb{P} .*

Proof. We prove by induction that $G/\gamma_n G$ has \mathbb{P} . The case $n = 2$ is trivial. Assume that $G/\gamma_{n-1} G$ has \mathbb{P} . By definition of an extendable property $G_{ab} \otimes \cdots \otimes G_{ab}$ has \mathbb{P} and with the Hall-epimorphism we see that $\gamma_{n-1} G/\gamma_n G$ has \mathbb{P} . Now the induction assumption together with the central extension

$$\gamma_{n-1} G/\gamma_n G \twoheadrightarrow G/\gamma_n G \twoheadrightarrow G/\gamma_{n-1} G$$

implies that $G/\gamma_n G$ has \mathbb{P} .

In particular the property holds for $G = G/\gamma_{c+1} G$ where c is the nilpotency class of G . \square

Theorem 4.23. *Every subgroup of a finitely generated nilpotent group is finitely generated.*

Proof. The property “having every subgroup finitely generated” is extendable: It is true for all finitely generated abelian groups, so points 1 and 2 of the definition are trivially satisfied. Let $A \twoheadrightarrow G \twoheadrightarrow Q$ be a central extension and assume that every subgroup of A and Q is finitely generated. Let H be a subgroup of G . Then $H \cap A$ is finitely generated and so is $H/H \cap A \cong HA/A$ because the right side is a subgroup of Q . Therefore the extension $H \cap A \twoheadrightarrow H \twoheadrightarrow H/H \cap A$ implies that H is finitely generated.

If G is finitely generated then $G_{ab} = G/G'$ is also fg. Thus the last theorem implies the statement of this theorem. \square

Corollary 4.24. *If G is nilpotent and finitely generated then G has a normal series*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$$

such that all G_i/G_{i-1} are cyclic.

Proof. The quotients of a central series are abelian and by the last theorem finitely generated. Therefore they decompose into cyclic groups. So it is possible to take a refinement of that series with cyclic factor groups. \square

5 Polycyclic Groups

Definition 5.1. A group with a normal series of finite length whose factor groups are cyclic is called *polycyclic*.

Examples 5.1.

1. By Theorem 4.24 every finitely generated nilpotent group is polycyclic.
2. $G = \mathbb{Z} \rtimes \mathbb{Z}$ where the action is defined by $1 \cdot x = -x$ is polycyclic but not nilpotent since $Z(G) = 1$.
3. $C_3 \twoheadrightarrow S_3 \twoheadrightarrow C_2$ is a group extension and therefore S_3 is polycyclic, but it is not nilpotent.

Theorem 5.2. *Every polycyclic group is finitely generated. The class of polycyclic groups is closed under taking subgroups and homomorphic images and under forming extensions. In particular every subgroup of a polycyclic group is finitely generated.*

Proof. By taking preimages of the quotients in the series one sees easily that all polycyclic groups are finitely generated.

Let $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$ be a normal series with cyclic quotients and $H \leq G$. Then $1 = G_0 \cap H \triangleleft G_1 \cap H \triangleleft \cdots \triangleleft G_r \cap H = H$ has cyclic quotients because there exists a monomorphism $(G_i \cap H)/(G_{i-1} \cap H) \hookrightarrow G_i/G_{i-1}$ and the image is cyclic. Therefore any subgroup of a polycyclic group is polycyclic. In a similar way one can show that the class of polycyclic groups is also closed under taking homomorphic images and forming extensions. \square

In a similar way to 4.24 one can prove the following:

Theorem 5.3. *A group G is polycyclic if and only if G is solvable and every subgroup of G is finitely generated.*

As a consequence the following inclusions hold:

$$\begin{aligned} \{\text{fg abelian groups}\} &\subseteq \{\text{fg nilpotent groups}\} \\ &\subseteq \{\text{polycyclic groups}\} \subseteq \{\text{fg solvable groups}\}. \end{aligned}$$

While properties of groups are often extensible across the first three classes, an extension to the last class is often impossible.

For polycyclic groups the length of a decomposition with cyclic factor groups is in general not unique. However the following statement holds:

Theorem 5.4. *In a polycyclic group G the number of infinite factor groups in a normal series with cyclic factor groups is independent of the series and hence is an invariant of the group. It is called the Hirsch² length or number (Hirschlänge in German).*

Proof. The theorem follows from two observations:

² Kurt Hirsch

1. By Schreier's refinement theorem 3.2 any two normal series with cyclic factors have isomorphic refinements.
2. Any refinement of a series with cyclic factors has the same number of infinite cyclic factors as the original series: If $H \triangleleft K$ and K/H is infinite-cyclic, i.e. $K/H \cong \mathbb{Z}$. Let $H \triangleleft L \triangleleft K$ such that $H \subsetneq L \subsetneq K$. Then L/H has to be isomorphic to a subgroup of \mathbb{Z} and is therefore of the form $m\mathbb{Z}$ which is infinite cyclic. On the other hand $K/L \cong \mathbb{Z}/m\mathbb{Z}$ is finite cyclic. \square

Definition 5.5. A polycyclic group G is called *infinite-cyclic* or *poly- \mathbb{Z}* if G is trivial or if it has a normal series consisting only of infinite cyclic factors.

Lemma 5.6. *The class of poly- \mathbb{Z} groups is closed under forming subgroups.*

Theorem 5.7. *Let G be an infinite polycyclic group. Then:*

1. G contains a normal subgroup of finite index that is poly- \mathbb{Z} .
2. G contains a nontrivial normal Abelian subgroup that is torsion-free.

Proof.

1. Let $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$ be a normal series with cyclic factor groups. We will prove by induction on n that G_n contains a subgroup with the desired properties. This is obvious for $n = 0$.

Assume that G_{n-1} contains $N \triangleleft_f G_{n-1}$ with N poly- \mathbb{Z} . Let M be a subgroup of N such that $M \triangleleft_{char} M$ and $[G_{n-1} : M] < \infty$. Then M is a normal subgroup of G_n and by the lemma M is poly- \mathbb{Z} .

We have a group extension

$$G_{n-1} \twoheadrightarrow G_n \twoheadrightarrow G_n/G_{n-1}$$

where the last group is cyclic. If G_n/G_{n-1} is finite, then M is the desired subgroup.

Otherwise assume $G_n/G_{n-1} = \langle G_{n-1}x \rangle \cong \mathbb{Z}$. Let $H = M\langle x \rangle$ (H is a subgroup of G_n because M is normal).

H is poly- \mathbb{Z} : $M \triangleleft M\langle x \rangle = H$ and therefore $H/M = \langle Mx \rangle \cong \mathbb{Z}$. Because M is poly- \mathbb{Z} it follows that H is poly- \mathbb{Z} .

$[G_n : H] < \infty$: Let Ma_1, \dots, Ma_k be all cosets of M in G_{n-1} . We will show that Ha_1, \dots, Ha_k comprises all cosets of H in G_n . Let $g \in G_n$, $g = x^i g'$ with $g' \in G_{n-1}$. Then $g' = ma_j$ with $m \in M$, $j \in \{1, \dots, k\}$. Therefore $g = x^i ma_j \in Ha_j$.

Let $P \leq H$, $P \triangleleft_f G_n$. P is the desired subgroup.

2. By 1. G has $N \triangleleft_f G$, N poly- \mathbb{Z} . N is solvable. Let l be the length of the derived series of N . Then $N^{(l)} = 1$ but $N^{(l-1)} \neq 1$. Therefore $N^{(l-1)}$ is abelian, torsion-free (because N is) and normal in G (because it is characteristic in N).

\square

6 Free Groups

Let G be generated by X and $f: X \rightarrow H$ be an arbitrary map into a group H . Then in general there need not exist an extension of f to a homomorphism $G \rightarrow H$. However, this would be a very convenient property of the group G . Therefore one defines:

Definition 6.1. Let X be a set and $f: X \rightarrow F$ a function from X into a group F . Then F is called *free* on X if for every group H and every function $g: X \rightarrow H$ there exist a unique homomorphism $\phi: F \rightarrow H$ such that the diagram

$$\begin{array}{ccc} X & \xrightarrow{f} & F \\ & \searrow g & \downarrow \phi \\ & & H \end{array}$$

commutes.

Example 6.1. \mathbb{Z} is free on $\{1\}$.

Theorem 6.2. Let $X \neq \emptyset$. Then there exists a group F and a function $f: X \rightarrow F$ such that F is free on X .

Proof. We will now construct the group F as equivalence classes of words. A *word* is a formal string $x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_r^{\epsilon_r}$ where $r \geq 1$, $x_i \in X$, $\epsilon_i \in \{\pm 1\}$. We will also need the *empty word* 1. On the set of words we define a multiplication by concatenation and the *inverse of a word* $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_r^{\epsilon_r}$ by $w^{-1} = x_r^{-\epsilon_r} \dots x_1^{-\epsilon_1}$. We identify two words w, v if w can be obtained by deleting or adding xx^{-1} or $x^{-1}x$ for some $x \in X$. Then the transitive and symmetric hull of this relation is an equivalence relation \sim on the set of words over X . Let F be the set of equivalence classes for this relation and define a multiplication on F by $[v][w] = [vw]$. Then F is a group (with identity element $[1]$ and inverse $[w]^{-1} = [w^{-1}]$) which is free on F with $f: X \rightarrow F: x \mapsto [x]$. \square

Usually one identifies $x \in X$ with $[x]$ such that $X \subseteq F$. A word is called *reduced* when it does not contain xx^{-1} or $x^{-1}x$ for any $x \in X$. Every equivalence class has a unique reduced representative. Any non-identity element of F can therefore be uniquely written in the *normal form* $x_1^{m_1} x_2^{m_2} \dots x_r^{m_r}$ with $x_i \in X$, $x_i \neq x_{i+1}$ and $m_i \in \mathbb{Z} \setminus \{0\}$.

Theorem 6.3. Let $X \subseteq G$. If every $g \in G \setminus \{1\}$ has a unique representation $g = x_1^{m_1} \dots x_r^{m_r}$, $x_i \neq x_{i+1}$, $x_i \in X$, $m_i \in \mathbb{Z} \setminus \{0\}$ then F is free on X .

Equivalently if $x_1^{m_1} \dots x_r^{m_r}$ with $x_i \neq x_{i+1}$, $x_i \in X$, $m_i \in \mathbb{Z} \setminus \{0\}$ is never equal to 1, then F is free on X .

Example 6.2. Let $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. We will show that $\langle A, B \rangle \leq \text{Gl}_2(\mathbb{C})$ is free on $\{A, B\}$ (where $\text{Gl}_2(\mathbb{C})$ are the invertible 2×2 -matrices over \mathbb{C}). To do this consider the homomorphism

$$\begin{array}{ccc} \text{Gl}_2(\mathbb{C}) & \longrightarrow & \text{Symm}(\mathbb{C}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & f(z) = \frac{az+b}{cz+d} \end{array}$$

where $\text{Symm}(\mathbb{C})$ is the group of bijections of \mathbb{C} . This map is of course not injective. The functions in its image are called *Möbius transformations* or *fractional linear transformations*. Under this homomorphism A maps to $\alpha(z) = z + 2$ and B maps to $\beta(z) = \frac{z}{2z+1}$. We will show that $\langle \alpha, \beta \rangle$ is free on $\{\alpha, \beta\}$.

Notice that for every $k \in \mathbb{Z}$ the function α^k maps the interior of the unit disk \mathbb{D} into the exterior of \mathbb{D} and β^k maps the exterior of \mathbb{D} into $\mathbb{D} \setminus \{0\}$. Then any composition of the form $\alpha^k \cdots \beta^l \alpha^n$ maps the interior of \mathbb{D} into the exterior and is therefore not 1. Similarly $\beta^k \cdots \alpha^l \beta^n \neq 1$ because it maps the exterior into the interior. $\beta^l \cdots \alpha^n(0) \neq 0$, so it is not the identity map and $\alpha^l \cdots \beta^n \neq 1$ since it maps 0 into the exterior. The last theorem shows that $\langle \alpha, \beta \rangle$ is free on $\{\alpha, \beta\}$ and therefore $\langle A, B \rangle$ must be free on $\{A, B\}$.

Theorem 6.4. *Every group is isomorphic to a quotient of a free group.*

Proof. Let G be any group and $X \subseteq G$ such that $G = \langle X \rangle$ (such a set X must always exist since $G = \langle G \rangle$). Let F be the free group on X .

$$\begin{array}{ccc} X & \xrightarrow{\subseteq} & F \\ & \searrow \subseteq & \downarrow \phi \\ & & G \end{array}$$

The universal property of a free group implies the existence of an epimorphism $\phi: F \rightarrow G$. Then $G \cong F/\ker \phi$. \square

Example 6.3. Let D_n be the dihedral group of order $2n$. Then then the *presentation* of D_n is $\langle a, b \mid b^2 = 1, bab^{-1} = a^{-1}, a^n = 1 \rangle$ which means the free group on $\{a, b\}$ factored by the smallest normal subgroup containing $\{a^2, bab^{-1}a, a^n\}$. Here a represents the “smallest” rotation and b a reflection.

Theorem 6.5 (Projective Property of Free Groups). *Let F be a free group, G, Q arbitrary groups, $\epsilon: G \twoheadrightarrow Q$ an epimorphism and $\phi: F \rightarrow Q$ a homomorphism. Then there exists a homomorphism $\psi: F \rightarrow G$ such that the following diagram commutes:*

$$\begin{array}{ccc} & F & \\ \psi \swarrow & \downarrow \phi & \\ G & \xrightarrow{\epsilon} & Q \end{array}$$

Proof. For every $q \in Q$ let $g_q \in G$ such that $\epsilon(g_q) = q$. Let F be free on X . Define a function $g: X \rightarrow G$ by $g(x) = g_{\phi(x)}$ and extend it to a homomorphism $\psi: F \rightarrow G$. \square

Definition 6.6. Let $N \xrightarrow{\iota} G \xrightarrow{\epsilon} Q$ be a group extension. If there exists a homomorphism $\sigma: Q \rightarrow G$ such that $\epsilon \circ \sigma = \text{id}_Q$ then σ is called a *splitting* and one says that the extension *splits*.

Remark 6.7. If an extension of the above form splits then $G \cong N \rtimes Q$.

Theorem 6.8. *Let $N \rightarrow G \xrightarrow{\epsilon} F$ be a group extension where F is free. Then the extension splits.*

Proof. Use the last theorem to get $\psi = \sigma$ from

$$\begin{array}{ccc} & & F \\ & \swarrow \sigma & \parallel \\ G & \xrightarrow{\epsilon} & F \end{array}$$

□

7 Residual Finiteness

Definition 7.1. Let \mathbb{P} be a group theoretic property. A group G is said to be *residually* \mathbb{P} if for any $g \in G$, $g \neq 1$ there exists a group H and an epimorphism $\phi: G \twoheadrightarrow H$ such that H has property \mathbb{P} and $\phi(g) \neq 1$.

Equivalently G is residually \mathbb{P} if and only if for any $g \in G$, $g \neq 1$ there exists $N \triangleleft G$ such that $g \notin N$ and G/N has property \mathbb{P} .

In particular G is *residually finite* if for any $g \in G$, $g \neq 1$ there exists $N \triangleleft_f G$ such that $g \notin N$ or equivalently if there exists $H \leq_f G$ such that $g \notin H$.

Examples 7.1.

- Any finite group is residually finite.
- \mathbb{Z} is residually finite: Let $n \in \mathbb{Z} \setminus \{0\}$ and p be a prime such that $p \nmid n$. Then $n \notin p\mathbb{Z} \leq_f \mathbb{Z}$.
- Let G_1, \dots, G_n be residually finite groups. Then $G_1 \times \dots \times G_n$ is residually finite. (Exercise)

The above examples and the classification of finitely generated abelian groups yield:

Theorem 7.2. *Any finitely generated abelian group is residually finite.*

Another class of residually finite groups are the polycyclic groups:

Theorem 7.3. *If G is polycyclic, then G is residually finite.*

Proof. Let $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_r = G$ be a normal series in G such that G_n/G_{n-1} is cyclic for all $1 \leq n \leq r$. We will prove by induction on n that G_n is residually finite. This is clear for $n = 1$ as G_1 is cyclic and therefore either finite or isomorphic to \mathbb{Z} .

Assume that G_{n-1} is residually finite and let $g \in G_n$, $g \neq 1$. Consider the group extension $G_{n-1} \twoheadrightarrow G_n \twoheadrightarrow G_n/G_{n-1}$. There are two cases:

First suppose $g \notin G_{n-1}$. Then $G_{n-1}g$ is a nontrivial element of G_n/G_{n-1} which is cyclic and thus residually finite. So there exists $\bar{H} \leq_f G_n/G_{n-1}$ such that $G_{n-1}g \notin \bar{H}$. By the correspondence theorem there exists $H \leq_f G_n$ with $\bar{H} = H/G_{n-1}$ and $g \notin H$.

Next suppose $g \in G_{n-1}$. Since G_{n-1} is residually finite by the induction hypothesis, we can find $K \leq_f G_{n-1}$ such that $g \notin K$. If G_n/G_{n-1} is finite then $[G_n : K] < \infty$ and we are done. So assume that G_n/G_{n-1} is infinite cyclic and let $G_n/G_{n-1} = \langle G_{n-1}x \rangle$. Since G_{n-1} is finitely generated, K contains a subgroup N which is characteristic in G_{n-1} such that $[G_{n-1} : N] < \infty$. Then N is normal in G_n and $L = N\langle x \rangle \leq G_n$. We will show that L is the subgroup we are looking for:

- $g \notin L$: Suppose that $g \in L$. Then $g = nx^i$ for some $n \in N, i \in \mathbb{Z}$. Since $N \leq G_{n-1}$ and $g \in G_{n-1}$ this implies $x^i \in G_{n-1}$ and therefore $i = 0$ and $g \in N$ which is a contradiction to $g \notin N$.
- $[G_n : L] < \infty$: Let Na_1, \dots, Na_k be the cosets of N in G_{n-1} . Take any $y \in G_n$ then for some $z \in G_{n-1} y = x^i z = x^i na_j \in La_j$ for some $n \in N, j \in \{1, \dots, k\}$. Therefore $[G_n : L] \leq k$. \square

In general it is not possible to extend properties of G to $\text{Aut}(G)$. However the following result does just that.

Theorem 7.4. *Let G be finitely generated and residually finite. Then $\text{Aut}(G)$ is residually finite.*

Proof. Let $\alpha \in \text{Aut}(G), \alpha \neq 1$. Then there exists $g \in G$ such that $\alpha(g) \neq g$. Let $x = \alpha(g)g^{-1} \neq 1$. Because G is residually finite, there exists $H \leq_f G$ such that $x \notin H$. Since G is finitely generated, H contains a subgroup $N \triangleleft_{char} G$ with $[G : N] < \infty$.

Notice that any $\beta \in \text{Aut}(G)$ induces an automorphism $\bar{\beta}$ of G/N defined by $Ny \mapsto N\beta(y)$ (this works because N is characteristic). The map $\text{Aut}(G) \rightarrow \text{Aut}(G/N) : \beta \mapsto \bar{\beta}$ is a homomorphism. Let Γ be the kernel of this homomorphism: $\Gamma = \{\beta \in \text{Aut}(G) : \bar{\beta} = \text{id}_{G/N}\}$. The sequence $\Gamma \rightarrow \text{Aut}(G) \rightarrow \text{Aut}(G/N)$ is exact and therefore $\text{Aut}(G)/\Gamma$ is isomorphic to $\text{Aut}(G/N)$. Since G/N is finite, so is its automorphism group and thus $[\text{Aut}(G) : \Gamma] < \infty$.

From $\alpha(g)g^{-1} = x \notin N$ it follows that $N\alpha(g) \neq Ng$ and therefore $\bar{\alpha}(Ng) \neq Ng$, i.e. $\alpha \notin \Gamma$. \square

Definition 7.5. A group G is called *hopfian* if it is not isomorphic to any of its proper quotients.

Equivalently G is hopfian if any epimorphism $\phi : G \twoheadrightarrow G$ is an isomorphism.

Heinz Hopf conjectured that any finitely generated group is hopfian. However the next example shows that this is false.

Example 7.2. Let H be the following multiplicative matrix group:

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 2^k & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z} \left[\frac{1}{2}\right], k \in \mathbb{Z} \right\}.$$

By example 4.1.3 this group is solvable. One can show that it is generated by the three matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. A is in the center of H and therefore the subgroups $\langle A \rangle$ and $\langle A^2 \rangle$ are normal in H . Let ϕ be the automorphism of H defined by

$$\phi \left(\begin{pmatrix} 1 & a & b \\ 0 & 2^k & c \\ 0 & 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & a & 2b \\ 0 & 2^k & 2c \\ 0 & 0 & 1 \end{pmatrix}.$$

Further define $\bar{\phi}: H/\langle A \rangle \rightarrow H/\langle A^2 \rangle$ by $\langle A \rangle h \mapsto \langle A^2 \rangle \phi(h)$. This is well-defined because $\phi(A) = A^2$ and is actually an isomorphism. Since $\langle A^2 \rangle \leq \langle A \rangle$ the isomorphism theorem yields

$$H/\langle A \rangle \cong (H/\langle A^2 \rangle) / (\langle A \rangle / \langle A^2 \rangle).$$

Therefore $G = H/\langle A^2 \rangle$ is a finitely generated solvable group that is isomorphic to a proper quotient.

Theorem 7.6. *Any finitely generated and residually finite group is hopfian.*

Lemma 7.7. *Let G be finitely generated and F a finite group. Then there are only finitely many homomorphisms $G \rightarrow F$.*

Proof. Let $G = \langle X \rangle$, $|X| < \infty$. Then any homomorphism $G \rightarrow F$ is completely determined by a map $X \rightarrow F$ and there are only finitely many of these maps. \square

Proof of the theorem. Suppose G is finitely generated and residually finite but not hopfian. So there exists an epimorphism $\phi: G \twoheadrightarrow G$ such that $\ker \phi \neq 1$. Let $x \in \ker \phi$, $x \neq 1$. Since G is residually finite there exists $\psi: G \rightarrow F$ such that F is a finite group and $\psi(x) \neq 1$.

We will show that $\psi\phi^n \neq \psi\phi^m$ for $m > n$. This yields infinitely many homomorphisms, contradicting that G is finitely generated. Since ϕ^n is always onto, there exists $y \in G$ such that $\phi^n(y) = x$. Then $\psi\phi^n(y) = \psi(x) \neq 1$ but $\psi\phi^m(y) = \psi\phi^{m-n}\phi^n(y) = \psi\phi^{m-n}(x) = \psi(1) = 1$. \square

7.1 Residual p -Groups

Theorem 7.8. *Any finitely generated torsion-free Abelian group is residually a finite p -group for all primes p .*

Proof. \mathbb{Z} has this property and if G_1, \dots, G_n are residually a finite p -group, then $G_1 \times \dots \times G_n$ is too. (Details are left as an exercise.) \square

One might be tempted to extend the last theorem to poly- \mathbb{Z} groups. However by the next example this is not possible.

Example 7.3. Let $G = \langle a, b \mid bab^{-1} = a^{-1} \rangle = \mathbb{Z} \rtimes \mathbb{Z}$ (see example 5.1.2). We will show that G is not residually a finite 3-group. Let $\phi: G \twoheadrightarrow F$ by any epimorphism from G into a finite 3-group. We will show that $\phi(a) = 1$. Since $\langle a \rangle$ is normal in G it follows that $\langle \phi(a) \rangle \triangleleft F$ and therefore $C_F(\phi(a)) \triangleleft F$. Applying ϕ to $b^2ab^{-2} = a$ yields $\phi(b)^2 \in C_F(\phi(a)) \triangleleft F$. Since $|F/C_F(\phi(a))|$ is a power of

three and thus relatively prime to 2 already $\phi(b)$ must be in $C_F(\phi(a))$. By the definition of the centralizer

$$\phi(a) = \phi(b)\phi(a)\phi(b)^{-1} = \phi(bab^{-1}) = \phi(a^{-1}).$$

So $\phi(a)^2 = 1$ and because F is a 3-group this can only happen when $\phi(a) = 1$.

Remark 7.9. If one looks closely at the example above one sees that the essential point is that there exists an element of finite order in $\phi(G)$ for every ϕ . It is possible to use essentially the same argument to show that any group which is not torsion-free cannot be residually a finite p -group for all primes p .

Theorem 7.10. *If G is a finitely generated torsion-free nilpotent group, then G is residually a finite p -group for all primes p .*

Proof. Let p be any prime. We will use induction on the nilpotency class of G . If $\text{nil } G = 1$ then G must be a free finitely generated Abelian group and therefore has the desired property by the theorem above. Let $\text{nil } G > 1$ and consider the extension $Z(G) \twoheadrightarrow G \twoheadrightarrow G/Z(G)$. For any $x \in G$ we have to consider two cases:

First let $x \notin Z(G)$. Let \bar{x} be the image of the natural epimorphism $G \twoheadrightarrow G/Z(G)$. By the induction hypothesis there exists $\phi: G/Z(G) \twoheadrightarrow F$ such that F is a finite p -group and $\phi(\bar{x}) \neq 1$. So we are done.

On the other hand when $x \in Z(G)$ things are more complicated: By our assumptions the order of x is not finite and therefore $x \notin \langle x^p \rangle \triangleleft G$ (the normality follows from the fact the x is in the center of G). Since $G/\langle x^p \rangle$ is a finitely generated nilpotent group it is polycyclic and in particular residually finite. Denote the image of x in this quotient by \bar{x} . Let $\psi: G/\langle x^p \rangle \twoheadrightarrow F$ such that F is finite and $\psi(\bar{x}) \neq 1$. F must be nilpotent because $G/\langle x^p \rangle$ is. By theorem 4.16 F is the direct product of its Sylow subgroups. Let F_p be a Sylow p -subgroup of F . Then there exists a projection map $\pi: F \twoheadrightarrow F_p$. Composing all our homomorphism we get an epimorphism $G \twoheadrightarrow G/\langle x^p \rangle \twoheadrightarrow F \twoheadrightarrow F_p$ where x is first mapped to \bar{x} then some element of order p in F and finally to a nontrivial element of F_p . The last group is a p -group. \square

Theorem 7.11. *Let G be polycyclic and residually a finite p -group for all primes p . Then G must be torsion-free and nilpotent.*

Proof. By remark 7.9, G must be torsion-free.

Since G is polycyclic there exists some $i \in \mathbb{N}$ such that $\gamma_i G / \gamma_{i+1} G$ is finite: If this were not true, then everyone of these quotients would contain a \mathbb{Z} -factor and one could construct a normal series with cyclic factors such that the number of \mathbb{Z} -factors exceeded the Hirsch number.

Let p be any prime and suppose that $\gamma_i G \neq 1$. Let $\phi: G \twoheadrightarrow F$ be an epimorphism such that F is a finite p -group and $\phi(\gamma_i G) \neq 1$. Then for every k , ϕ induces an epimorphism $\phi_k: \gamma_k G \twoheadrightarrow \gamma_k F$. Taking quotients ϕ induces an epimorphism $\bar{\phi}: \gamma_i G / \gamma_{i+1} G \twoheadrightarrow \gamma_i F / \gamma_{i+1} F$. By the definition of ϕ , $\gamma_i F \neq 1$ and since F must be nilpotent (by theorem 4.13) $\gamma_i F \neq \gamma_{i+1} F$. Thus $\gamma_i F / \gamma_{i+1} F \neq 1$ and it is a p -group. Therefore p divides $|\gamma_i G / \gamma_{i+1} G|$ and since p was arbitrary, $|\gamma_i G / \gamma_{i+1} G| = \infty$. This is a contradiction to our choice of i and thus $\gamma_i G = 1$ and G is nilpotent. \square

Corollary 7.12. *A polycyclic group is residually a finite p -group for all primes p if and only if it is torsion-free and nilpotent.*

Theorem 7.13. *Let F be a free group. Then F is residually a finite p -group for all primes p .*

Proof. Let F be free on X and let $f \in F \setminus \{1\}$. Then $f = x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r}$ for some $r \in \mathbb{N}$, $x_u \in X$ with $x_u \neq x_{u+1}$, and $m_u \in \mathbb{Z} \setminus \{0\}$. Take $n \in \mathbb{N}$ such that $p^n \nmid m_1 \cdots m_r$. Let M be the multiplicative group of upper unitriangular $(r+1) \times (r+1)$ -matrices over $\mathbb{Z}/p^n\mathbb{Z}$. Then M is a finite p -group. Further for $1 \leq u, v \leq r+1$ let E_{uv} be the $(r+1) \times (r+1)$ -matrix with 1 in the (u, v) -entry and zeros elsewhere. An easy calculation shows $E_{uv}E_{vw} = E_{uw}$ and $E_{uv}E_{u'v'} = 0$ for $v \neq u'$.

Now for $1 \leq j \leq r$ let

$$A_j = \prod_{x_u=x_j} (1 + E_{u(u+1)}) = 1 + \sum_{x_u=x_j} E_{u(u+1)},$$

because products of two $E_{u(u+1)}$ matrices will always be zero as $x_{u+1} \neq x_u$. Further calculation shows

$$A_j^{m_j} = 1 + m_j \sum_{x_u=x_j} E_{u(u+1)}.$$

Define a homomorphism $\theta: F \rightarrow M$ by $\theta(x_j) = A_j$ for $1 \leq j \leq r$ and $\theta(x) = 1$ for all other $x \in X$. We will show that $\theta(f) \neq 1$: $\theta(f) = \theta(x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r}) = A_1^{m_1} A_2^{m_2} \cdots A_r^{m_r}$. Multiply this out and express it as a linear combination of the E_{kl} s. Then the coefficient of $E_{1(r+1)}$ is $m_1 \cdots m_r \neq 1$ in $\mathbb{Z}/p^n\mathbb{Z}$ and therefore $\theta(f) \neq 1$. \square

8 HNN Extensions

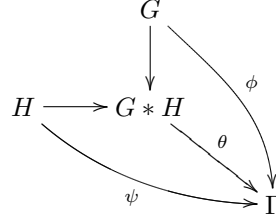
Definition 8.1. Let G and H be any groups and form the set \mathcal{W} of words of elements of G and H with the usual product and inversion of words. Call two words v, w equivalent ($v \sim w$) if w can be obtained from v by a finite sequence of operations of the following types:

1. Replacing $g_1 g_2$ by g if $g_1 g_2 = g$ in G .
Replacing $h_1 h_2$ by h if $h_1 h_2 = h$ in H .
2. The reverse of operation 1.
3. Omitting or adding 1_G or 1_H .

The set $G * H := \mathcal{W} / \sim$ with the operation defined by $[v][w] = [vw]$ is a group called the *free product of G and H* .

The natural maps $G \rightarrow G * H$ and $H \rightarrow G * H$ are injections.

Theorem 8.2 (Universal Property of $G * H$). *If $\phi: G \rightarrow \Gamma$ and $\psi: H \rightarrow \Gamma$ are any homomorphisms into a group Γ then there exists a unique homomorphism $\theta: G * H \rightarrow \Gamma$ such that the diagram*



commutes.

The property can be used to define the free product.

Definition 8.3. Let A and B be subgroups of G and $\phi: A \rightarrow B$ an isomorphism. The group

$$\text{HNN}(G, \phi) = G * \langle t \rangle / t^{-1}at = \phi(a) \quad \forall a \in A,$$

where $t \notin G$ and the factorization is by the smallest normal subgroup containing $t^{-1}at\phi(a)^{-1}$ for all $a \in A$, is called the *HNN extension* of G .

In the extension the isomorphism ϕ can be interpreted as conjugation by t .

Definition 8.4. For any monomorphism $\phi: G \rightarrow G$ the group

$$G_\phi = \text{AHNN}(G, \phi) = G * \langle t \rangle / t^{-1}gt = \phi(g) \quad \forall g \in G$$

is called an *ascending HNN extension*.

Remark 8.5.

- If ϕ is an automorphism, then $G_\phi = G \rtimes \langle t \rangle$.
- In the AHNN extension the relations $t^{-1}gt = \phi(g)$ and $gt = t\phi(g)$ hold. Therefore every element in G_ϕ can be written as t^kgt^{-l} for $k, l \geq 0$.

In general if G is residually finite, G_ϕ does not have to be residually finite. However this property holds for some important types of groups.

Theorem 8.6 (Wise, Hsu, 2002). *If G is polycyclic then G_ϕ is residually finite.*

Theorem 8.7 (Sapir, Borisov, 2005). *If G is a finitely generated free group then G_ϕ is residually finite.*

The remainder of this course is used to prove theorem 8.6. This will be done by first showing that G_ϕ being residually finite is equivalent to ϕ possessing a certain property and then that polycyclic groups imply this property.

Definition 8.8. An endomorphism $\phi: G \rightarrow G$ is said to have property \mathbb{P} if for every $g \in G$ there exists $N \triangleleft_f G$ such that for all $i \geq 0$: $\phi^i(g) \in N$ if and only if $\phi^i(g) = 1$.

Lemma 8.9. *If ϕ is a monomorphism then ϕ has property \mathbb{P} if and only if for all $g \in G \setminus \{1\}$ there exists $N \triangleleft_f G$ such that $\phi^i(g) \notin N \forall i \geq 0$.*

Theorem 8.10. *Let G be finitely generated and $\phi: G \rightarrow G$ a monomorphism. Then G_ϕ is residually finite if and only if ϕ has property \mathbb{P} .*

Proof. First assume that G_ϕ is residually finite. Let $g \in G, g \neq 1$. Then there exists $M \triangleleft_f G_\phi$ with $g \notin M$. Let $N = M \cap G$. Now suppose $\phi^i(g) \in N$ for some $i \geq 0$. In G_ϕ , ϕ is equivalent to conjugation and thus $\phi^i(g) = t^{-i}gt^i \in N \subseteq M$. Since M is normal this implies $g \in M$, a contradiction.

The second direction of the theorem is more difficult to prove. Assume that property \mathbb{P} holds. Let $x \in G_\phi, x \neq 1$. By the remark above $x = t^kgt^{-l}$ for some $g \in G, k, l \geq 0$.

First assume that $g \neq 1$. Since ϕ has property \mathbb{P} there exists $N \triangleleft_f G$ such that $\phi^i(g) \notin N \forall i \geq 0$. By proposition 2.9 we may assume without loss of generality that $\phi(N) \subseteq N$. Then

$$N \subseteq \phi^{-1}(N) \subseteq \phi^{-2}(N) \subseteq \dots$$

where $\phi^{-i}(N) = \{y \in G : \phi^i(y) \in N\}$. Let $M = \bigcup_{i=0}^{\infty} \phi^{-i}(N) \leq G$. By our choice of $N, g \notin M$ and since $\phi^{-i}(N) \triangleleft G, N \leq M \triangleleft_f G$. Additionally $\phi(M) \subseteq M$. Therefore there exists an induced homomorphism $\bar{\phi}: G/M \rightarrow G/M$ which is injective ($Mx \in \ker \bar{\phi} \Rightarrow \phi(x) \in M \Rightarrow \phi(x) = \phi^{-i}(z)$ for some $z \in N \Rightarrow x = \phi^{-i-1}(z) \Rightarrow x \in M$). As G/M is finite $\bar{\phi}$ is actually an isomorphism.

Form the semidirect product $G/M \rtimes \langle \bar{t} \rangle$ with the action defined by $\bar{t}My\bar{t}^{-1} = \bar{\phi}^{-1}(My)$. Remember that in $G_\phi, t^{-1}yt = \phi(y) \forall y \in G$. Hence there exists $\theta: G_\phi \rightarrow G/M \rtimes \langle \bar{t} \rangle$ mapping $y \mapsto My \forall y \in G$ and $t \mapsto \bar{t}$. Let $H = \theta^{-1}(\langle \bar{t} \rangle)$. Since $\langle \bar{t} \rangle$ has finite index, $H \leq_f G_\phi$ and since $g \notin H$ but $t \in H, x = t^kgt^{-l} \notin H$. So this case is done.

Now assume that $g = 1$. Then $x = t^k$ for $k \in \mathbb{Z} \setminus \{0\}$. There exists an epimorphism $\epsilon: G_\phi \rightarrow \mathbb{Z}$ such that $\epsilon(G) = 0$ and $\epsilon(t) = 1$ (because this respects the relation $t^{-1}gt = \phi(g)$). Let $A \leq_f \mathbb{Z}$ such that $n \notin A$. Then $H = \epsilon^{-1}(A) \leq_f G_\phi$ and $x = t^k \notin H$.

In both cases we have found a subgroup H such that $x \notin H \leq_f G_\phi$. Therefore G_ϕ is residually finite. \square

Remark 8.11. The first part of the proof does not use the assumption that G is finitely generated. Therefore the implication “ G_ϕ is residually finite $\Rightarrow \phi$ has property \mathbb{P} ” is always true.

We can now apply this to all kinds of groups to prove that their AHNN extensions must be residually finite.

Example 8.1. If $\phi: \mathbb{Z} \rightarrow \mathbb{Z}$ is a monomorphism then ϕ has property \mathbb{P} .

Proof. Any monomorphism of \mathbb{Z} has the form $\phi(x) = kx$ for some $k \in \mathbb{Z}$. Let $x \in \mathbb{Z}, x \neq 0$. Then $\phi^i(x) = k^i x$. Let p be a prime such that $\gcd(p, k) = \gcd(p, x) = 1$. Then $k^i x \notin p\mathbb{Z}$ for all $i \geq 0$. \square

Corollary 8.12. *Every group of the form $\langle a, b \mid b^{-1}ab = a^k \rangle$ with $k \in \mathbb{Z}$ is isomorphic to an AHNN extension of \mathbb{Z} and therefore is residually finite.*

Theorem 8.13. *If A is a finitely generated abelian group and $\phi : A \rightarrow A$ is an endomorphism, then ϕ has property \mathbb{P} .*

Proof. First, assume that ϕ is one-to-one. Let $A = F \oplus \bar{A}$, where F is finite and $\bar{A} \cong \mathbb{Z}^n$ is torsion-free. Let $a \in A$, $a \neq 0$. We need a subgroup of finite index that misses $\phi^i(a)$ for all $i \geq 0$. Let \bar{a} be the \bar{A} -portion of a . If $\bar{a} = 0$, use \bar{A} as the subgroup.

Suppose $\bar{a} \neq 0$. Let p be a prime, such that p does not divide all components of \bar{a} and $p \nmid \det \bar{\phi}$ (where $\bar{\phi} : \bar{A} \rightarrow \bar{A}$ is the \mathbb{Z} -module monomorphism induced by ϕ). Then for all $i \geq 0$, p does not divide all components of $\bar{\phi}^i(\bar{a})$. Thus $\bar{\phi}^i(\bar{a}) \notin p\bar{A}$ and hence $\phi^i(a) \notin pA$. pA is the desired subgroup.

If ϕ is not one-to-one, consider the chain $\ker \phi \subseteq \ker \phi^2 \subseteq \ker \phi^3 \subseteq \dots$. Let $C = \bigcup_{j=1}^{\infty} \ker \phi^j \leq A$. Then $\phi(C) \subseteq C$ and hence ϕ induces a monomorphism $\bar{\phi} : A/C \rightarrow A/C$ which has property \mathbb{P} by the first case. Let $a \in A$, $a \neq 0$. We need a subgroup $D \leq_f A$ such that $\phi^i(a) \in D \Leftrightarrow \phi^i(a) = 0$.

If $a \notin C$ apply the fact that $\bar{\phi}$ has property \mathbb{P} and obtain D by the correspondence theorem. Otherwise $\phi^k(a) = 0$ for some $k > 0$ and thus $\phi^i(a) = 0$ for all $i \geq k$. By the residual finiteness of A there exists $D \leq_f A$ such that $\phi^i(a) \notin D$ for all $0 \leq i < k$. Then D is the desired subgroup. \square

Theorem 8.14 (Big Theorem of This Lecture). *If G is polycyclic and $\phi : G \rightarrow G$, the ϕ has property \mathbb{P} .*

This theorem together with theorem 8.10 finally proves theorem 8.6.

Proof. We will use induction on the derived length of G . The base case is covered by the last theorem. Look at the group extension $G' \twoheadrightarrow G \twoheadrightarrow G_{ab}$. Then $\phi(G') \subseteq G'$ and thus ϕ induces maps $\phi_{ab} : G_{ab} \rightarrow G_{ab}$ and $\bar{\phi} : G' \rightarrow G'$ which both have property \mathbb{P} (by the base case resp. by induction).

Let $g \in G$, $g \neq 1$. If $\phi^k(g) = 1$ for some k , then $\phi^i(g) = 1$ for all $i \geq k$. Let $N \triangleleft_f G$ such that $\phi^i(g) \notin N$ for $0 \leq i < k$. Then N is the desired subgroup.

Otherwise $\phi^i(g) \neq 1$ for all $i \geq 0$. If $\phi^i(g) \notin G'$ for all i , apply the fact that ϕ_{ab} has property \mathbb{P} and use the correspondence theorem to get the desired subgroup.

Now suppose the $\phi^k(g) \in G'$ for some k . Then $\phi^i(g) \in G'$ for all $i \geq k$. Let k be the smallest nonnegative integer such that $\phi^k(g) \in G'$. $\bar{\phi}$ has property \mathbb{P} and therefore there exists $M \triangleleft_f G'$ such that $\phi^i(g) \notin M$ for all $i \geq k$. By a homework exercise, since G_{ab} is polycyclic: $\exists N_1 \triangleleft_f G$ such that $N_1 \cap G' \leq M$. Then $\phi^i(g) \notin N_1$ for all $i \geq k$.

If $k = 0$, then N_1 is the subgroup we are looking for. Otherwise let $N_2 \triangleleft_f G$ such that $\phi^i(g) \notin N_2$ for $i \in \{0, \dots, k-1\}$. Then $N = N_1 \cap N_2$ is the desired subgroup. \square

We will conclude this lecture with two examples of ascending HNN-extensions of residually finite groups that are not residually finite.

Examples 8.2.

1. Let $\mathbb{Z}_2 = \left\{ \frac{m}{n} : n \text{ odd}, m, n \in \mathbb{Z} \right\}$ be the localization of \mathbb{Z} in 2. This group is not finitely generated but it is residually a 2-group: Let $x \in \mathbb{Z}_2$, $x \neq 0$. Take $k > 0$ such that $2^k \nmid x$ in \mathbb{Z}_2 . Then $x \notin 2^k \mathbb{Z}_2$. In particular, \mathbb{Z}_2 is residually finite. The only finite homomorphic images of \mathbb{Z}_2 are 2-groups. Let $\phi: \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, $\phi(x) = 2x$. Then one cannot find a subgroup of finite index missing $\phi^i(1) = 2^i$ for all $i \geq 0$. Therefore, by remark 8.11, $\text{AHNN}(\mathbb{Z}_2, \phi)$ is not residually finite.
2. Let $A = \bigoplus_{\mathbb{Z}} \mathbb{Z}_2$ and $Q = \bigoplus_{\mathbb{Z}} \mathbb{Z} \rtimes \mathbb{Z} = \langle t, x : [t^k x t^{-k}, t^l x t^{-l}] = 1 \rangle$ with $t = ((0), 1)$ and $x = ((\delta_{i0})_{i=-\infty}^{\infty}, 0)$. Form an action of Q on A such that t shifts one entry to the right and x multiplies the i -th component by $2i+1$. Then the group $G = A \rtimes Q$ is solvable since Q is solvable and A is abelian. Further it is 3-generated and residually finite (lemma: if N and Q are residually finite, the $N \rtimes Q$ is residually finite). Define a monomorphism $\phi: G \rightarrow G$ by $\phi((a_i), q) = ((2a_i), q)$. Then by the same reason as in the first example, ϕ does not have property \mathbb{P} .

Index

- abelianization, 8
- action, 4
- ascending central series, 9
- ascending HNN extension, 25
- center, 2
- central extension, 10
- central series, 9
 - ascending, 9
 - descending, 9
 - lower, 9
 - upper, 9
- centralizer, 2
- characteristic subgroup, 6
- class formula, 3
- closed under forming central extensions, 10
- closed under forming extensions, 9
- commutator, 2
- commutator subgroup, 8
- conjugacy class, 3
- conjugation, 2–4
- core, 6
- correspondence theorem, 4
- derived length, 8
- derived subgroup, 8
- derives series, 8
- descending central series, 9
- dihedral group, 4, 19
- exact sequence, 8
- extendable property, 14
- extension, 8
 - central, 10
 - HNN, 25
- finitely generated abelian group, 4
- fractional linear transformation, 19
- free group, 18
 - projective property, 19
- free product, 24
 - universal property, 25
- group extension, 8
 - splitting, 19
- Hall-epimorphism, 13
- Heisenberg Group, 12
- Hirsch length, 16
- Hirsch number, 16
- HNN extension, 25
 - ascending, 25
- hopfian group, 21
- infinite-cyclic, 17
- isomorphism theorem, 3
- lower central series, 9
- Möbius transformation, 19
- metabelian, 8
- nilpotency class, 10
- nilpotent group, 10
- normal core, 6
- normal series, 7
 - isomorphic, 7
 - refinement, 7
- normalizer, 3
- Π -divisible, 15
- Π -group, 15
- p -subgroup, 3
- poly- \mathbb{Z} , 17
- polycyclic group, 16
- presentation of a group, 19
- product
 - direct, 4
 - free, 24
 - semidirect, 4
- projective property of free groups, 19
- refinement, 7
- residually finite, 20
- residually \mathbb{P} , 20
- Schreier's Refinement Theorem, 7
- semidirect product, 4
- solvable group, 8
- splitting extension, 19
- subnormal, 11
- Sylow p -subgroup, 3
- Sylow's theorems, 3
- tensor product, 5

torsion subgroup, 4
torsion-free, 4

universal property
 free product, 25

upper central series, 9

word, 18, 24
 inverse, 18
 normal form, 18
 reduced, 18

Zassenhaus' lemma, 7