GROUP THEORY MATH 4106/5106, WINTER 2007

FREE GROUPS. LECTURE NOTES.
THIS PART IS A MODIFICATION OF NOTES WRITTEN BY A.MYASNIKOV [3]

Contents

1. Free groups

1.1. **Definition, bases.** Let S be an arbitrary set. We define the free group $F(S)$ generated by S, as follows. A *word* w in S is a finite sequence of elements which we write as $w = y_1 \dots y_n$, where $y_i \in S$. The number n is called the *length of the word* w, we denote it by $|w|$. The empty sequence of elements is also allowed. We denote the empty word by e and set its length to be $|e| = 0$. Consider the set $S^{-1} = \{s^{-1} \mid s \in S\}$ where s^{-1} is just a formal expression. We call s^{-1} the *formal inverse of* s. The set

$$S^{\pm 1} = S \cup S^{-1}$$

is called *the alphabet of* F, and an element $y \in S^{\pm 1}$ of this set is called a *letter*. By s^1 we mean s, for each $s \in S$.

An expression of the type

$$w = s_{i_1}^{\epsilon_1} \dots s_{i_n}^{\epsilon_n} \quad (s_{i_j} \in S;\ \epsilon_j \in \{1, -1\})$$

is called a *group word in* S. So a group word in S is just a word in the alphabet $S^{\pm 1}$. A group word $w = y_1 \dots y_n$ $(y_i \in S^{\pm 1})$ is *reduced* if the following condition holds. Whenever $y_i \in S$, neither y_{i-1} nor y_{i+1} is the formal inverse of y_i, for each $i = 1, \dots, n$; by y_0 and y_{n+1} one means empty words. In other words, w contains no subword of the type ss^{-1} or $s^{-1}s$, for all $s \in S$. We assume also that the empty word is reduced.

Let G be a group, and let $S \subseteq G$ be a set of elements of G. In this case, by the formal inverse s^{-1} of $s \in S$ we mean the inverse of s in G. Every group word $w = s_{i_1}^{\epsilon_1} \dots s_{i_n}^{\epsilon_n}$ in S determines a unique element from G which is equal to the product $s_{i_1}^{\epsilon_1} \dots s_{i_n}^{\epsilon_n}$ of the elements $s_{i_j}^{\epsilon_j} \in G$. In particular, the empty word e determines the identity 1 of G.

Definition 1.1. A group G is called a *free group* if there exists a generating set S in G such that every non-empty reduced group word in S defines a non-trivial element of G. If this is the case, then one says that G is *freely generated by* S (or that G is free on S), and S is called a *free basis of* G.

It follows from the definition that if G is a group freely generated by S, then different reduced words in S define different elements in G.

1.2. **Construction of a free group with basis S.** Let S be an arbitrary set. To construct a free group with basis S, we need to describe a *reduction process* which allows one to obtain a reduced word from an arbitrary word. An *elementary reduction* of a group word w consists of deleting a subword of the type yy^{-1} where $y \in S^{\pm 1}$ from w. For instance, let $w = uyy^{-1}v$ for some words u and v in S. Then the elementary reduction of w with respect to the given subword yy^{-1} results in the word uv. In this event we write

$$uyy^{-1}v \to uv$$

A *reduction of* w (or a *reduction process starting at* w) consists of consequent applications of elementary reductions starting at w and ending at a reduced word:

$$w \to w_1 \to \cdots \to w_n, \quad (w_n \text{ is reduced})$$

The word w_n is termed a *reduced form of* w. In general, there may be different possible reductions of w. Nevertheless, it turns out that all possible reductions of w end up with the same reduced form. To see this we need the following lemma.

Lemma 1.2. *For any two elementary reductions $w \to w_1$ and $w \to w_2$ of a group word w in S there exist elementary reductions $w_1 \to w_0$ and $w_2 \to w_0$, so that the following diagram commutes.*

$$\begin{tikzcd} & w \arrow[dl] \arrow[dr] & \\ w_1 \arrow[dr] & & w_2 \arrow[dl] \\ & w_0 & \end{tikzcd}$$

Proof. Let $\lambda_1 \colon w \to w_1$ and $\lambda_2 \colon w \to w_2$ be elementary reductions of a word w. We distinguish the following two cases.

(1) Disjoint reductions. In this case $w = u_1y_1y_1^{-1}u_2y_2y_2^{-1}u_3$ where $y_i \in S^{\pm 1}$ and λ_i deletes the subword $y_iy_i^{-1}$ $(i = 1, 2)$. Then

$$\lambda_2 \circ \lambda_1 \colon w \to u_1u_2y_2y_2^{-1}u_3 \to u_1u_2u_3 \tag{1}$$

$$\lambda_1 \circ \lambda_2 \colon w \to u_1y_1y_1^{-1}u_2u_31 \to u_1u_2u_3 : \tag{2}$$

Hence the lemma holds.

(2) Overlapping reductions. In this case $y_1 = y_2$ and w takes on the following form $w = u_1yy^{-1}yu_2$. Then

$$\lambda_2 \colon w = u_1y(y^{-1}y)u_2 \to u_1yu_2 \quad \text{and} \tag{3}$$

$$\lambda_1 \colon w = u_1(yy^{-1})yu_2 \to u_1yu_2 \tag{4}$$

and the lemma holds.

□

Proposition 1.3. *Let w be a group word in S. Then any two reductions of w:*

$$w \to w_0' \to \cdots \to w_n' \quad \textit{and} \tag{5}$$

$$w \to w_0'' \to \cdots \to w_m'' \tag{6}$$

result in the same reduced form, in other words, $w_n' = w_m''$.

Proof. Our proof is by induction on $|w|$. If $|w| = 0$ then w is reduced and there is nothing to prove. Let now $|w| > 1$. Then by Lemma 1.2, there are elementary reductions $w_0' \to w_0$ and $w_0'' \to w_0$. Consider a reduction process for $w_0 \to w_1 \to \cdots \to w_k$. This corresponds to the following diagram:

$$\begin{tikzcd}
 & & w \arrow[dl] \arrow[dr] & & \\
 & w_0' \arrow[dl] \arrow[dr] & & w_0'' \arrow[dl] \arrow[dr] & \\
w_1' \arrow[d] & & w_0 \arrow[d] & & w_1'' \arrow[d] \\
\cdots \arrow[d] & & w_1 \arrow[d] & & \cdots \arrow[d] \\
w_n' & & \cdots \arrow[d] & & w_m'' \\
 & & w_k & &
\end{tikzcd}$$

By the induction hypothesis, all reduced forms of the word w_0' are equal to each other, as well as all reduced forms of w_0''. Since w_k is a reduced form of both w_0' and w_0'', we have that $w_n' = w_k = w_m''$ as desired. This proves the proposition. □

For a group word w, by $\bar{w}$ we denote the unique reduced form of w. Let $F(S)$ be the set of all reduced words in S. For $u, v \in F(S)$ we define multiplication $u \cdot v$ as follows:

$$u \cdot v = \overline{uv}.$$

Theorem 1.4. *The set $F(S)$ forms a group with respect to the multiplication "$\cdot$". This group is free on S.*

Proof. The multiplication defined above is associative:

$$(u \cdot v) \cdot w = u \cdot (v \cdot w)$$

for all $u, v, w \in F(S)$. To see this it suffices to prove that $\overline{(\overline{uv})w} = \overline{u(\overline{vw})}$ for given u, v, w. Observe that each one of the reduced words $\overline{(\overline{uv})w}$ and $\overline{u(\overline{vw})}$ can be obtained form the word uvw by a sequence of elementary reductions, hence by Proposition 1.3,

$$\overline{\overline{uv}w} = \overline{uvw} = \overline{u\overline{vw}}.$$

Clearly, the empty word e is the identity in $F(S)$ with respect to the multiplication defined as above, i.e.,

$$e \cdot w = w \cdot e$$

for every $w \in F(S)$. For this reason we usually denote e by 1. Let $w = y_1 \dots y_n$ with $y_i \in S^{\pm 1}$ be a word in S. Then the word $w^{-1} = y_n^{-1} \dots y_1^{-1}$ is also reduced and

$$w \cdot w^{-1} = y_1 \dots y_n \bar{y}_n^{-1} \dots y_1^{-1} = 1.$$

Hence w^{-1} is the inverse of w. This shows that $F(S)$ satisfies all the axioms of a group. Notice that S is a generating set of $F(S)$ and every non-empty reduced word $w = s_{i_1}^{\epsilon_1} \dots s_{i_n}^{\epsilon_n}$ in $S^{\pm 1}$ defines a non-trivial element in $F(S)$ (the word w itself). Hence S is a free basis of $F(S)$, so that $F(S)$ is freely generated by S. □

1.3. **Word problem and conjugacy problem.**

Definition 1.5. (Cyclically reduced word) Let $w = y_1 y_2 \dots y_n$ be a word in the alphabet $S^{\pm 1}$. The word w is cyclically reduced, if w is reduced and $y_n \neq y_1^{-1}$.

Example 1.6. *The word $w = s_1 s_3 s_2^{-1}$ is cyclically reduced, whereas neither $u = s_1 s_2^{-1} s_1 s_3 s_2 s_1^{-1}$, nor $v = s_1 s_3^{-1} s_3 s_2^{-1}$ is a cyclically reduced word.*

If a word w is not cyclically reduced, then one can cyclically reduce it, by the following procedure. If w is not reduced, then we can reduce w by a sequence of elementary reductions and get the reduced form $\bar{w}$ of w. If $\bar{w} = y_1 y_2 \dots y_k$ is not cyclically reduced, then $y_k = y_1^{-1}$. We eliminate the first and the last letter of $\bar{w}$ and keep doing so, until we obtain a cyclically reduced word. Note that if $\bar{w} = y_1 y_2 \dots y_{k-1} y_1^{-1}$ and $w' = y_2 \dots y_{k-1}$ is obtained from $\bar{w}$ by eliminating y_1 and $y_k = y_1^{-1}$, then $\bar{w}$ and w' represent different elements in $F(S)$, that are conjugate:

$$\bar{w} = y_1 w' y_1^{-1}.$$

Apparently, it follows from Proposition 1.3 that a cyclically reduced form of w is unique.

Example 1.7. *If we cyclically reduce the word $u = s_1 s_2^{-1} s_1 s_3 s_2 s_1^{-1}$, then we obtain $u' = s_1 s_3$. Note that $u = (s_1 s_2^{-1}) u' (s_1 s_2^{-1})^{-1}$, so that u and u' are conjugate in $F(S)$.*

Free groups and subgroups of free groups have very good algorithmic properties. Some of these properties require more developed techniques, and we prove them later on. Solvability of the word and conjugacy problems can be easily derived from the definition of a free group.

Lemma 1.8. *The word and the conjugacy problem in a free group are solvable.*

Proof. Observe that there is an (obvious) algorithm to compute both reduced and cyclically reduced forms of a given word w.

Our algorithm to solve the word problem is based on Proposition 1.3: a word w represents the trivial element in $F(S)$ if and only if the reduced form of w is the empty word.

Now, let $\tilde{u}$ and $\tilde{v}$ be two words in the alphabet S, and let u and v be the cyclically reduced forms of these words. Then $\tilde{u} = g_u u g_u^{-1}$ and $\tilde{v} = g_v v g_v^{-1}$ for some g_u and g_v in $F(S)$. Therefore, $\tilde{u}$ and $\tilde{v}$ represent conjugate elements in $F(S)$ if and only if u and v are conjugate in $F(S)$. Indeed,

$$\tilde{u} = g\tilde{v}g^{-1} \Leftrightarrow g_u u g_u^{-1} = g g_v v g_v^{-1} g^{-1} \Leftrightarrow u = (g_u^{-1} g g_v) v (g_u^{-1} g g_v)^{-1}.$$

Thus, to solve the conjugacy problem, we can assume that we are given two elements $u = y_1 \dots y_n$ and $v = z_1 \dots z_m$ in cyclically reduced forms, and these reduced forms are distinct: $y_1 \dots y_n \neq z_1 \dots z_m$ (for if they are equal, then they are conjugate by the trivial element, and we are done). Assume that u and v are conjugate in $F(S)$. In other words, we assume that there is a reduced word $g = s_1 \dots s_k$ so that the following equality holds:

$$y_1 \dots y_n = s_1 \dots s_k z_1 \dots z_m s_k^{-1} \dots s_1^{-1}.$$

Since two elements of $F(S)$ are equal if and only if their reduced forms are the same, and $y_1 \dots y_n$ is a cyclically reduced word, we conclude that the word in the right-hand side is not reduced. Hence, either $s_k^{-1} = z_1$, or $s_k = z_m$. Without loss of generality, we can assume that $s_k = z_1^{-1}$, so that we can eliminate the pair $s_k z_1$ by an elementary reduction.

If $k = 1$, then $s_1^{-1} = z_1$, and we have that

$$y_1 \dots y_n = s_1 z_1 z_2 \dots z_m s_1^{-1} = s_1 s_1^{-1} z_2 \dots z_m s_1^{-1} = z_2 \dots z_m s_1^{-1} = z_2 \dots z_m z_1,$$

so that the word $y_1 \dots y_n$ is obtained from the word $z_1 \dots z_m$ by cyclic permutation of the letters. Since the word $z_1 \dots z_m$ is cyclically reduced, each cyclic permutation of it is reduced. In particular, $y_1 \dots y_n$ and $z_2 \dots z_m z_1$ are reduced forms of the same element in $F(S)$, hence these two words are the same.

For $k > 1$, we proceed by induction on the length k of the conjugating element. Indeed, it suffices to observe that

$$\begin{aligned} y_1 \dots y_n &= s_1 \dots s_{k-1} s_k z_1 \dots z_m s_k^{-1} s_{k-1}^{-1} \dots s_1^{-1} \\ &= s_1 \dots s_{k-1} z_2 \dots z_m z_1 s_{k-1}^{-1} \dots s_1^{-1}, \end{aligned}$$

where $z_2 \dots z_m z_1$ is a (cyclically reduced) cyclic permutation of $z_1 \dots z_m$. □

1.4. **The universal property of free groups.**

Theorem 1.9. *Let G be a group with a generating set $S \subset G$. Then G is freely generated by S if and only if G has the following universal property. Every map $\phi\colon S \to H$ from S into a group H can be extended to a unique homomorphism $\tilde{\phi}\colon G \to H$ so that the diagram below commutes*

$$\begin{tikzcd} S \arrow[r, hook] \arrow[dr, "\phi"'] & G \arrow[d, "\tilde{\phi}"] \\ & H \end{tikzcd}$$

(here $S \hookrightarrow G$ is the inclusion of S into G).

Proof. Let G be a group freely generated by S and let $\phi\colon S \to H$ be a map from S into a group H. Since G is freely generated by S, every element $g \in G$ is defined by a unique reduced word in $S^{\pm 1}$. Let

$$g = s_{i_1}^{\epsilon_1} \cdot \dots \cdot s_{i_n}^{\epsilon_n} \quad (s_{i_j} \in S,\ \epsilon_i \in \{1, -1\}).$$

We set $\tilde{\phi}(g)$ to be

$$\tilde{\phi}(g) = (\phi(s_{i_1}))^{\epsilon_1} \dots (\phi(s_{i_n}))^{\epsilon_n}. \tag{7}$$

We claim that $\tilde{\phi}$ is a homomorphism. Indeed, let $g, h \in G$ be so that

$$g = y_1 \dots y_n z_1 \dots z_m \text{ and } h = z_m^{-1} \dots z_1^{-1} y_{n+1} \dots y_k$$

are the corresponding reduced words in S, where $y_i, z_j \in S^{\pm 1}$ and $y_n \neq y_{n+1}^{-1}$ (we allow the subwords $y_1 \dots y_n$, $z_1 \dots z_m$ and $y_{n+1} \dots y_k$ to be empty). Then

$$gh = y_1 \dots y_n y_{n+1} \dots y_k$$

is a reduced word in S that presents gh. Now,

$$\begin{aligned} \tilde{\phi}(gh) &= \tilde{\phi}(y_1) \dots \tilde{\phi}(y_n) \tilde{\phi}(y_{n+1}) \dots \tilde{\phi}(y_k) \\ &= \tilde{\phi}(y_1) \dots \tilde{\phi}(y_n) \tilde{\phi}(z_1) \dots \tilde{\phi}(z_m) \tilde{\phi}(z_m)^{-1} \dots \tilde{\phi}(z_1)^{-1} \tilde{\phi}(y_{n+1}) \dots \tilde{\phi}(y_k) \\ &= \tilde{\phi}(g) \tilde{\phi}(h) \end{aligned}$$

Hence $\tilde{\phi}$ is a homomorphism. Clearly, $\tilde{\phi}$ extends ϕ and the corresponding diagram commutes. Observe that any homomorphism $\tilde{\phi}\colon G \to H$ that makes the diagram commutative, must satisfy the equalities (7), so $\tilde{\phi}$ is unique.

This shows that G satisfies the required universal property. Suppose now that a group G with a generating set S satisfies the universal property. Take $H = F(S)$ and define a map $\phi\colon S \to H$ by $\phi(s) = s$ for each $s \in S$. Then by the universal property ϕ extends to a unique homomorphism $\tilde{\phi}\colon G \to F(S)$. Let w be a non-empty reduced group word on S. Then w defines an element g in G for which $\tilde{\phi}(g) = w \in F(S)$. Hence $\tilde{\phi}(g) \neq 1$ and consequently $g \neq 1$ in G. This shows that G is a free group on S. This proves the theorem. □

Observe that the argument above implies the following result, which we state as a corollary.

Corollary 1.10. *Let G be a free group on S. Then the identical map $S \to S$ extends to an isomorphism $G \to F(S)$.*

This corollary allows us to identify a free group freely generated by S with the group $F(S)$. In what follows we usually refer to the group $F(S)$ as to the free group on S.

1.5. **The Isomorphism problem.**

Theorem 1.11. *Let G be freely generated by a set S, and let H be freely generated by a set U. Then $G \cong H$ if and only if $|S| = |U|$.*

Proof. First, assume that $|S| = |U|$. Fix a bijection $\sigma\colon S \to U$. By the universal property, σ extends to a homomorphism $\tilde{\sigma}\colon F(S) \to F(U)$. Similarly, the bijection $\tau = \sigma^{-1}\colon U \to S$ extends to a homomorphism $\tilde{\tau}\colon F(U) \to F(S)$. Let $\nVdash_G \in Aut(G)$ and $\nVdash_H \in Aut(H)$ denote the identity automorphisms of G and H, respectively. The equalities $\tilde{\tau} \circ \tilde{\sigma} = \nVdash_G$ and $\tilde{\sigma} \circ \tilde{\tau} = \nVdash_H$ imply that the kernel of $\tilde{\sigma}$ is trivial and that $\tilde{\sigma}$ is an onto homomorphism. Altogether, we have that $\tilde{\sigma}$ is an isomorphism, and so $F(S) \cong F(U)$. By Corollary 1.10, $G \cong F(S)$ and $H \cong F(U)$, so that $G \cong H$.

Now, let $G \cong H$. Let $K \subseteq G$ be the subgroup generated by $\{g^2 \mid g \in G\}$. Let $k = g_1^2 g_2^2 \dots g_n^2$, and let $g \in G$. Observe that

$$\begin{aligned} gkg^{-1} &= gg_1^2g_2^2 \dots g_n^2 g^{-1} = (gg_1^2g^{-1})(gg_2^2g^{-1}) \dots (gg_n^2g^{-1}) \\ &= (gg_1g^{-1})^2(gg_2g^{-1})^2 \dots (gg_ng^{-1})^2 \in K, \end{aligned}$$

so that $K \lhd G$. Also observe that for all $g, b \in G$ we have that

$$[g, b] = gbg^{-1}b^{-1} = g^{-1}g^2b^2b^{-1}g^{-1}b^{-1} = (g^{-1}g^2b^2g)(g^{-1}b^{-1})^2 \in K,$$

hence G/K is abelian. Let $\eta : G \to G/K$ be the natural homomorphism. Whereas $s^2 \in K$ obviously, $s \notin K$, for all $s \in S$, because $|k| \geq 2$ for all $k \in K$; we conclude that $\eta(s) \in G/K$ has the order 2. We claim that for any $s_1, s_2 \in S$ such that $s_1 \neq s_2$, the images $\eta(s_1) \neq \eta(s_2)$ are distinct. Indeed, by the way of contradiction, assume that $s_1s_2^{-1} = g^2$ for some $g \in G$. Since the word $s_1s_2^{-1}$ is reduced, $g = s_1y_1 \dots y_m s_2^{-1}$ for some $m \geq 0$ and $y_i \in$

$S^{\pm 1}$; in particular, g is cyclically reduced, hence $|g^2| \geq 4$, a contradiction. Therefore,

$$G/K \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{|S| \text{ times}}.$$

Similarly, one considers $P \lhd H$ generated by $\{h^2 \mid h \in H\}$. Since G and H are isomorphic, so are P and K, and $G/K \cong H/P$. The classification theorem for finite abelian groups implies that $|S| = |U|$. □

Corollary 1.12. *The isomorphism problem for finitely generated free groups is solvable.*

Exercise. If G and H are defined by presentations, where both generating sets are bases: $G = \langle S \mid - \rangle$ and $H = \langle U \mid - \rangle$, then there is an obvious algorithm to determine, whether or not G and H are isomorphic. Find an algorithm in the case, when $G = \langle S \mid - \rangle$ (so that G is freely generated by S) and $H = \langle U \mid R \rangle$ is a free group defined by the presentation with non-empty set R of relations.

1.6. **Embeddings of free groups.**

Definition 1.13. Let G be a free group on S. Then the cardinality of S is called *the rank of G*.

Sometimes we refer to a free group of rank n as to F_n. Notice that if $S \subseteq Y$, then the subgroup $\langle S \rangle$ generated by S in $F(Y)$ is itself a free group with basis S. This implies that if m and n are cardinals and $n \leq m$, then F_n can be embedded into F_m. We will show now that free groups of larger ranks can be embedded into free groups of smaller ranks.

We say that a group G *embeds* into a group H, if there is a monomorphism $\phi\colon G \to H$. If $\phi(G) \subsetneqq H$, then we say that G *properly embeds* into H and that ϕ is *a proper embedding.*

Proposition 1.14. *Any countable free group G can be embedded into a free group of rank* 2*.*

Proof. To prove the result it suffices to find a free subgroup of countable rank in a free group of rank 2. Let F_2 be a free group with a basis $\{a, b\}$. Denote

$$x_n = b^n a b^{-n} \ (n = 0, 1, 2, \dots)$$

and let $S = \{x_0, x_1, x_2, \dots\}$. We claim that S freely generates the subgroup $\langle S \rangle$ in F_2. Indeed, let

$$w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \dots x_{i_n}^{\epsilon_n}$$

be a reduced non-empty word in $S^{\pm 1}$. Then w can also be viewed as a word in $\{a, b\}$. Indeed,

$$w = b^{i_1} a^{\epsilon_1} b^{-i_1} b^{i_2} a^{\epsilon_2} b^{-i_2} \dots b^{i_n} a^{\epsilon_n} b^{-i_n}.$$

Since w is a reduced word in S, we have that either $i_j \neq i_{j+1}$, or $i_j = i_{j+1}$ and $\epsilon_j + \epsilon_{j+1} \neq 0$, for each $j = 1, 2, \ldots, n-1$. In either case, any reduction of w (as a word in $\{a, b\}$) does not affect a^{ϵ_j} and $a^{\epsilon_{j+1}}$ in the subword

$$b^{i_j} a^{\epsilon_j} b^{-i_j} b^{i_{j+1}} a^{\epsilon_{j+1}} b^{-i_{j+1}}$$

i.e., the literals a^{ϵ_j} and $a^{\epsilon_{j+1}}$ are present in the reduced form of w as a word in $\{a, b\}^{\pm 1}$. Hence the reduced form of w is non-empty, so $w \neq 1$ in F_2. Clearly, $\langle S \rangle$ is a free group of countable rank. □

1.7. **Examples and properties of free groups.** Whereas the construction of a free group in Section 1.2 may seem somewhat artificial, free groups occur as subgroups in many groups that exist in the "real life". The following lemma is often used in proofs of this kind.

Lemma 1.15. *(Ping-pong lemma) Let a group G, generated by a and b, act on a set X. Assume that there are two nonempty subsets A and B of X, so that $A \cap B = \emptyset$, and $a^n.B \subseteq A$ and $b^n.A \subseteq B$ for all integers $n \neq 0$. Then G is freely generated by a and b.*

Proof. Let w be a nonempty reduced word in the alphabet $a^{\pm 1}, b^{\pm 1}$. W.l.o.g., we can assume that w begins and ends with $a^{\pm 1}$, for if not then for m large enough a conjugate $w_1 = a^m w a^{-m}$ of w does, and $w = 1$ iff $w_1 = 1$. Let $w = a^{n_1} b^{m_1} \cdot a^{n_{k-1}} b^{m_{k-1}} a^{n_k}$, with $n_i, m_i \neq 0$. Then

$$\begin{aligned} w.B = & a^{n_1} b^{m_1} \cdot a^{n_{k-1}} b^{m_{k-1}} a^{n_k}.B \subseteq a^{n_1} b^{m_1} \cdot a^{n_{k-1}} b^{m_{k-1}}.A \subseteq \\ & a^{n_1} b^{m_1} \cdot a^{n_{k-1}}.B \subseteq \cdots \subseteq a^{n_1}.B \subseteq A. \end{aligned}$$

It follows that $w \neq 1$, and so a and b freely generate G. □

Corollary 1.16. *The matrices*

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

generate a free subgroup in $SL_2(\mathbb{Z})$.

Proof. Denote by $G = \langle A, B \rangle$ the subgroup of $SL_2(\mathbb{Z})$ generated by A and B. The group G acts on $X = \mathbb{R}^2$, and if we set $V = \{[x, y]^T \mid |x| < |y|\}$ and $W = \{[x, y]^T \mid |x| > |y|\}$, then $A^n.W \subseteq V$ and $B^n.V \subseteq W$, for all $n \neq 0$. By the Ping-pong lemma, G is freely generated by A and B. □

Definition 1.17. A group G is called *linear* if it can be embedded into a group of matrices $GL_n(\mathbb{P})$ for some integer $n \geq 1$ and some field $\mathbb{P}$.

Theorem 1.18. *A free group of countable rank is linear. In particular, any finitely generated free group is linear.*

Proof. The assertion is immediate from Corollary 1.16 and Proposition 1.14. □

Definition 1.19. A group G is called *residually finite* if for any nontrivial element $g \in G$ there exists a homomorphism $\phi\colon G \to H$ into a finite group H so that $\phi(g) \neq 1$.

Clearly, finite groups are residually finite, and subgroups of residually finite groups are residually finite.

Exercise. Prove that $SL_n(\mathbb{Z})$ is residually finite.

Theorem 1.20. *Free groups are residually finite.*

Proof. The assertion is immediate from Theorem 1.18 and the Exercise. □

2. Presentations of groups

The universal property of free groups allows one to describe arbitrary groups in terms of generators and relators. Let G be a group with a generating set S. By the universal property of free groups there exists a homomorphism $\varphi\colon F(S) \to G$ such that $\varphi(s) = s$ for $s \in S$. It follows that φ is onto, so by the first isomorphism theorem

$$G \simeq F(S)/ker(\varphi).$$

In this event $ker(\varphi)$ is viewed as the set of *relators* of G, and a group word $w \in ker(\varphi)$ is called a *relator* of G in generators S. If a subset $R \subset ker(\varphi)$ generates $ker(\varphi)$ as a normal subgroup of $F(S)$ then it is termed a *set of defining relations of G relative to S*. The pair $\langle S \mid R\rangle$ is called a *presentation of G*, it determines G uniquely up to isomorphism. The presentation $\langle S \mid R\rangle$ is *finite* if both sets S and R are finite. A group is *finitely presented* if it has at least one finite presentation. Presentations provide a universal method to describe groups.

Example 2.1. *Examples of finite presentations.*

1. $G = \langle s_1, \dots, s_n \mid [s_i, s_j],\ \forall 1 \le i < j \le n\rangle$ *is the free abelian group of rank* n.
2. $C_n = \langle s \mid s^n = 1\rangle$ *is the cyclic group of order* n.
3. *Both presentations* $\langle a, b \mid ba^2b^{-1}a^{-3}\rangle$ *and* $\langle a, b \mid ba^2b^{-1}a^{-3}, [bab^{-1}, a]\rangle$ *define the Baumslag-Solitar group* $BS(2,3)$ *(to be proved in Assignment 2).*

2.1. **Homomorphisms of groups.** If a group G is defined by a presentation, then one can try to find homomorphisms from G into other groups.

Lemma 2.2. *Let* $G = \langle S \mid R\rangle$ *be a group defined by a (finite) presentation with the set of relators* $R = \{r_j = y^{(j)}_{i_1} \dots y^{(j)}_{i_j} \mid y^{(j)}_i \in S^{\pm 1}, 1 \le j \le m\}$, *and let* H *be an arbitrary group. A map* $\psi\colon S^{\pm 1} \to H$ *extends to a homomorphism* $\tilde{\psi}\colon G \to H$, *if and only if* $\psi(r_j) = \psi(y^{(j)}_{i_1}) \dots \psi(y^{(j)}_{i_j}) = 1$ *in* H *for all* $r_j \in R$.

Proof. Define the map $\tilde{\psi}\colon G \to H$ by

$$\tilde{\psi}(y_{n_1} \dots y_{n_t}) = \psi(y_{n_1}) \dots \psi(y_{n_t}),$$

whenever $y_{n_i} \in S^{\pm 1}$ (cf. the proof of Theorem 1.9). If $\tilde{\psi}$ is a homomorphism, then obviously $\tilde{\psi}(r_j) = 1$ for all $r_j \in R$.

Now, assume that $\tilde{\psi}$ is defined as above, and that $\tilde{\psi}(r_j) = 1$ for all $r_j \in R$ Let η be the natural homomorphism from the free group $F(S)$ onto G, let $U = \psi(S^{\pm 1})$, and let $F(U)$ be the free group on U. There is a natural homomorphism λ from the free group $F(U)$ onto the subgroup H_1 of H generated by $U = \psi(S^{\pm 1})$ in H. By the universal property of free groups, the map $\psi\colon S^{\pm 1} \to U$ extends to a homomorphism $\alpha\colon F(S) \to F(U)$, so that the composition of homomorphisms $\lambda \circ \alpha$ is a homomorphism from $F(S)$ onto H_1:

$$\begin{tikzcd}
\alpha\colon F(S) \arrow[r] \arrow[d, "\eta"'] & F(U) \arrow[d, "\lambda"] \\
G & H
\end{tikzcd}$$

Let $g = y_{n_1} \dots y_{n_t} \in G$, where $y_{n_i} \in S^{\pm 1}$. Without loss of generality, we can assume that the word $w_g = y_{n_1} \dots y_{n_t}$ is reduced. We regard the word w_g as an element of $F(S)$, and define $\tilde{\psi}(g) = \lambda \circ \alpha(w_g)$. We only need to check that $\lambda \circ \alpha(w_g) = \lambda \circ \alpha(w_b)$, whenever $\eta(w_g) = \eta(w_b)$. Recall that $\eta(w_g) = \eta(w_b)$ if and only if $w_g = w_b w_k$, where $w_k \in ker(\eta)$. Our assumption on ψ implies that $\lambda \circ \alpha(w_k) = 1$ in H, so that $\lambda \circ \alpha(w_g) = \lambda \circ \alpha(w_b)$ indeed, and the map $\tilde{\psi}(g)$ is well defined. In other words, we define the images of elements of G in H to be equal to the images of representatives of left cosets of $F(S)$ with respect to the kernel of the natural homomorphism $\eta\colon F(S) \to G$. As we have just shown, the image of $g \in G$ does not depend on a choice of a representative in $F(S)$, hence our definition of the map $\tilde{\psi}$ is correct. It is immediate from the definition of $\tilde{\psi}$ that $\tilde{\psi}$ is a homomorphism. The assertion is proved. □

Let G be a group, by the *commutant* (or *derived subgroup*) G' of G we mean the subgroup generated by all the commutators $[g, b] = gbg^{-1}b^{-1}$ in G. Since $a[g, b]a^{-1} = [aga^{-1}, aba^{-1}]$, the commutant is a normal subgroup of G. The quotient G/G' is called the *abelianization* of G. This name is given to this quotient because G/G' is an abelian group.

For example, the abelianization of a free group F_n is the free abelian group of rank n. In general, if

$$G = \langle s_1, \dots, s_n \mid r_1, \dots, r_m \rangle, \quad \text{then}$$
$$G/G' = \langle s_1, \dots, s_n \mid r_1, \dots, r_m, [s_i, s_j](1 \leq i < j \leq n) \rangle$$

As the following corollary shows, the abelianization G/G' is the largest abelian quotient of G, in a sense.

Corollary 2.3. *Let H be an abelian quotient of G, and let $\nu\colon G \to G/G'$ and $\psi\colon G \to H$ be the natural homomorphisms. Then there is a homomorphism*

$\varphi\colon G/G' \to H$ so that the following diagram commutes:

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\psi"'] & G/G' \arrow[d, "\varphi"] \\ & H \end{tikzcd}$$

Proof. Let G be generated by $S = \{s_1, \dots, s_n\}$, then G/G' is generated by $\nu(S) = \{\nu(s_1), \dots, \nu(s_n)\}$. We still denote $\nu(s_i)$ by s_i, since we want to fix the alphabet $S^{\pm 1}$ for both G and G/G'. Hence, G/G' has the presentation above. Define a map $\varphi'\colon \nu(S) \to H$ by $\varphi'(s_i) = \psi(s_i)$ for all i. Observe that $\varphi'(r_j) = \psi(r_j) = 1$ in H, since ψ is a homomorphism and $r_j = 1$ in G. Also, $\varphi'([s_i, s_j]) = \psi([s_i, s_j]) = [\psi(s_i), \psi(s_j)] = 1$, since H is abelian. It follows now from Lemma 2.2 that the map φ' extends to a homomorphism from G/G' to H. □

2.2. **Tietze transformations.** As we have seen, a group can have many presentations. It turns out that all the presentations of G can be obtained from a given presentation

$$G = \langle a, b, c, \cdots \mid r_1, r_2, r_3, \dots \rangle \tag{8}$$

by a sequence of so-called *Tietze transformations.* These transformations, introduced by H. Tietze in 1908, are as follows:

(T1) If the words $p, q, \dots$ are derivable from $r_1, r_2, r_3, \dots$, then add $p, q, \dots$ to the defining relators in (8).

(T2) If some of the relators, say, $p, q, \dots$, listed among the defining relators $r_1, r_2, r_3, \dots$ are derivable from the others, delete $p, q, \dots$ from the defining relators in (8).

(T3) If $x, y \dots$ are any words in $a, b, c, \dots$, then adjoin the symbols $g, h, \dots$ to the generating symbols in (8) and adjoin the relations $g = x$, $h = y, \dots$ to the defining relators in (8).

(T4) If some of the defining relations in (8) take the form $g = x$, $h = y, \dots$, where $g, h, \dots$ are generators in (8) and $x, y \dots$ are words in the generators other than $g, h, \dots$, then delete $g, h, \dots$ from the generators, delete $g = x$, $h = y, \dots$ from the defining relations, and replace $g, h, \dots$ by $x, y \dots$ respectively, in the remaining defining relators in (8).

Theorem 2.4. *Given two presentations of a group G,*

$$G = \langle a_1, a_2, \cdots \mid r_1, r_2, \dots \rangle \tag{9}$$

and

$$G = \langle b_1, b_2, \cdots \mid p_1, p_2, \dots \rangle, \tag{10}$$

then (10) *can be obtained from* (9) *by a repeated application of the Tietze transformations (T1),(T2),(T3) and (T4).*

Proof. We only outline the idea of a proof here. The generators $b_1, b_2, \dots$ are elements of G, hence they can be expressed as words $b_1 = B_1(a_1, a_2, \dots)$,

$b_2 = B_2(a_1, a_2, \dots)$ in $a_1, a_2, \dots$. Use (T3) to adjoin the new generating symbols $b_1, b_2, \dots$ and adjoin the relations $b_1 = B_1(a_1, a_2, \dots)$, $b_2 = B_2(a_1, a_2, \dots)$ to the presentation (9). Now, one can adjoin the defining relations $p_1, p_2, \dots$ so as to get the presentation

$$G = \langle a_1, a_2, \dots, b_1, b_2, \cdots \mid r_1, r_2, \dots, p_1, p_2, \dots \rangle. \tag{11}$$

Express $a_1, a_2, \dots$ in terms of $b_1, b_2, \dots$ so as to express the relators $r_1, r_2, \dots$ in terms of $b_1, b_2, \dots$, and apply (T4) and (T2) to (11). One ends up with the presentation (10). □

Claim 2.5. *The presentation*

$$H = \langle x, y, z \mid y(xyz^{-1})^2 x, z(xyz^{-1})^3, [x, y], [y, z], [z, x] \rangle$$

defines the free abelian group of rank 2.

Proof. Let $A = \langle a, b \mid [a, b] \rangle$ be the free abelian group of rank two. We use the Tietze transformation (T3) to adjoin the new generators $x = ab$, $y = b^{-1}a$, $z = a^3$, so as to get the following presentation of A:

$$A \cong \langle a, b, x, y, z \mid [a, b], x = ab, y = b^{-1}a, z = a^3 \rangle.$$

Now, it follows from the relations in this latter presentation that $a = z(xy)^{-1}$ and $b = z(xy)^{-1}y^{-1} = z(yxy)^{-1}$, as well as $[x, y] = [y, z] = [x, z] = 1$; add these new relations to this presentation, using (T1).

Now, we use (T4) to eliminate a and b from the presentation:

$$A \cong \langle x, y, z \mid x = z(xy)^{-1} z(yxy)^{-1}, y = yxyz^{-1} z(xy)^{-1},$$
$$z = (z(xy)^{-1})^3, [x, y], [y, z], [x, z] \rangle.$$

The second relation is trivial, so that we can eliminate it (this is a particular case of (T2)). It can be readily seen that in this latter presentation of A the relators are cyclic permutations of the relators from the presentation of H. □

References

[1] W. Magnus, A. Carras, D. Solitar, *Combinatorial Group Theory*, 1966.

[2] R. Lyndon, P. Schupp, *Combinatorial Group Theory*, 1977.

[3] A. Myasnikov, *Lecture notes*, available at http://www.cs.gc.cuny.edu/ amyasnikov/