MT5824: Topics in Groups

Alex Levine

December 8, 2017

Chapter 1

Free Groups

1.1 Constructing Free Groups

Definition 1.1.1 Let X be a set and X^{-1} be another set, such that there exists a bijection called *invert*, denoted $\wedge^{-1}$ from X to X^{-1} and $X \cap X^{-1} = \emptyset$.

A *word* or *string* over X is a sequence of elements of $X \cup X^{-1}$. The set of all finite length words over X is denoted $W(X)$.

Remark 1.1.2 We have assumed, given X, that such an X^{-1} exists. This can be proved using set theory, but it is beyond the scope of the course.

Example 1.1.3 Let $X = \{a, b\}$, and $X^{-1} = \{a^{-1}, b^{-1}$. Define

$$\begin{aligned} \wedge^{-1} : X &\to X^{-1} \\ c &\mapsto c^{-1}. \end{aligned}$$

Note that $\wedge^{-1}$ is a bijection, and $X \cap X^{-1} = \emptyset$. We have

$$aba^{-1}aab^{-1}a \in W(X).$$

Observe $(a^{-1})^{-1} = a$.

Remark 1.1.4 Note that given a set X, there may be multiple possibilities for X^{-1}. To keep X^{-1} the same (at least notationally), we will use every symbol of X, superscripted with -1.

Definition 1.1.5 Let X be a set. Define the binary operation $\bullet$ by

$$\begin{aligned} \bullet : W(X) \times W(X) &\to W(X) \\ (v,\ w) &\mapsto vw \quad \text{(concatentation)}. \end{aligned}$$

Lemma 1.1.6 *Let X be a set. The pair*

$$(W(X),\ \bullet)$$

forms a monoid.

Proof The operation $\bullet$ clearly maps to elements of $W(X)$; the result of concatenating two finite lengths words over X is a finite length word over X.

Let $w_1,\ w_2,\ w_3 \in W(X)$ be

$$\begin{aligned} w_1 &= x_1 x_2 \cdots x_k, \\ w_2 &= y_1 y_2 \cdots y_l, \\ w_3 &= z_1 z_2 \cdots z_m, \end{aligned}$$

where $k,\ l,\ m \in \mathbb{N}_0$ and $x_i,\ y_i,\ z_i \in X \cup X^{-1}$ for all valid indices i. Then

$$\begin{aligned} w_1(w_2 w_3) &= x_1 \cdots x_k (y_1 \cdots y_l z_1 \cdots z_m) \\ &= x_1 \cdots x_k y_1 \cdots y_l z_1 \cdots z_m \\ &= (x_1 \cdots x_k y_1 \cdots y_l) z_1 \cdots z_m \\ &= (w_1 w_2) w_3, \end{aligned}$$

so $\bullet$ is associative.

Note that concatenating any word with the empty word does not change the word, so the empty word is the identity.

Definition 1.1.7 The monoid $(W(X),\ \bullet)$ is denoted $(X \sqcup X^{-1})^*$.

Definition 1.1.8 Let X be a set. A word

$$w_1 = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \in W(X),$$

for some $m \in \mathbb{N}_0$, is a *simple expansion* of

$$w_2 = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_i^{\varepsilon_i} x_{i+3}^{\varepsilon_{i+3}} \cdots x_m^{\varepsilon_m},$$

where $\varepsilon_i \in \{-1, 1\},\ x_{i+2} = x_{i+1},\ \varepsilon_{i+1} = -\varepsilon_{i+2}$. In addition we say w_1 is a *simple contraction* of w_2. We write $w_1 \searrow w_2$ and $w_2 \nearrow w_1$.

Example 1.1.9 Let $X = \{a, b\}$. The word $aba^{-1}abb^{-1}a^{-1}b^{-1}$ is a simple expansion of $abb^{-1}a^{-1}b^{-1}$ and also of $aba^{-1}aa^{-1}b^{-1}$.

Definition 1.1.10 Let X be a set. If there exists a finite chain of simple expansions and simple contractions taking a word $z_1 \in W(X)$ to $z_2 \in W(x)$, we say $z_1 \sim z_2$.

Lemma 1.1.11 *Let X be a set. The relation $\sim$ is an equivalence relation on $W(X)$.*

Proof Let X be a set. Let $z_1,\ z_2,\ z_3 \in W(X),\ a \in X$. We have

$$z_1 \sim z_1 a a^{-1} \sim z_1,$$

so $\sim$ is reflexive. Suppose $z_1 \sim z_2$. Consider the sequence of simple expansions and contractions that takes z_1 to z_2. If every simple expansion in this sequence is replaced with a simple contraction and vice versa, this will take z_2 to z_1, so $z_2 \sim z_1$ and $\sim$ is symmetric. Suppose, in addition, that $z_2 \sim z_3$. Concatenate the sequences of simple expansions and contractions that take z_1 to z_2 and vice versa. This will take z_1 to z_3, so $z_1 \sim z_3$ and $\sim$ is transitive.

Definition 1.1.12 Let X be a set. Define $\bullet_\sim$ on ${W(X)}\!\diagup\!{\sim}$ by

$$\begin{aligned}\bullet_\sim : {W(X)}\!\diagup\!{\sim} \times {W(X)}\!\diagup\!{\sim} &\to {W(X)}\!\diagup\!{\sim}\\ (([z_1],\ [z_2]) &\mapsto [z_1 \bullet z_2]\end{aligned}$$

Lemma 1.1.13 *The binary operation $\bullet_\sim$ is well-defined.*

Proof Let X be a set. Let $z_1,\ z_2 \in W(X)$. Let $w_1 \in [z_1],\ w_2 \in [z_2]$. We have

$$[w_1] \bullet_\sim [w_2] = [w_1 \bullet w_2].$$

We have $w_1 \sim z_1,\ w_2 \sim z_2$. Therefore

$$w_1 \bullet w_2 \sim z_1 \bullet w_2 \sim z_1 \bullet z_2,$$

and hence $[w_1 \bullet w_2] = [z_1 \bullet z_2]$ and $\bullet_\sim$ is well-defined.

Theorem 1.1.14 *The pair $\left({W(X)}\!\diagup\!{\sim},\ \bullet_\sim\right)$ forms a group.*

Proof By Lemma 1.1.6, we have that it is a monoid. Let

$$z = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k},$$

for some $k \in \mathbb{N}_0,\ x_i \in X \cup X^{-1},\ \varepsilon_i \in \{1, -1\}$ for valid indices i. Define

$$w = x_k^{-\varepsilon_k} \cdots x_1^{-\varepsilon_1}.$$

We have

$$\begin{aligned} wz &= x_k^{-\varepsilon_k} \cdots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1} x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \\ &= x_k^{-\varepsilon_k} \cdots x_2^{-\varepsilon_2} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \\ &= \cdots \\ &= x_k^{-\varepsilon_k} x_k^{\varepsilon_k} \\ &= \epsilon, \end{aligned}$$

and

$$\begin{aligned} zw &= x_1^{\varepsilon_1} \cdots x_{k-1}^{\varepsilon_{k-1}} x_k^{\varepsilon_k} x_k^{-\varepsilon_k} x_{k-1}^{-\varepsilon_{k-1}} \cdots x_1^{-\varepsilon_1} \\ &= x_1^{\varepsilon_1} \cdots x_{k-1}^{\varepsilon_{k-1}} x_{k-1}^{-\varepsilon_{k-1}} \cdots x_1^{-\varepsilon_1} \\ &= \cdots \\ &= x_1^{\varepsilon_1} x_1^{-\varepsilon_1} \\ &= \epsilon \end{aligned}$$

So w is the inverse of z and we have a group.

Definition 1.1.15 Let X be a set. The group $\left({W(X)}\!\diagup\!{\sim},\ \bullet_\sim\right)$ is called the *free group on X* and is denoted F_X.

Definition 1.1.16 Let G be a group. An element $g \in G$ is a *torsion* element, if $g^n = 1_G$, for some $n \in \mathbb{N}$. A group is *torsion-free* if the only torsion element of the group is the identity.

Example 1.1.17 Let X be a non-empty set. Let $w \in W(X)$ such that $w \not\sim \varepsilon$. Let $n \in \mathbb{N}$. Then

$$[w^n]_\sim = ([w]_\sim)^n \neq 1_{F_X}.$$

Hence $X \neq \emptyset \implies F_X$ is torsion free.

1.2 Free Bases

Definition 1.2.1 A subset X of a group F is called a *free basis* for F, if there is a function $\varphi : X \to G$, for some group G, such that φ can be extended uniquely to a group homomorphism $\tilde{\varphi} : F \to G$.

Lemma 1.2.2 *Let X be a set. The group F_X has free basis*

$$[X]_\sim := \{ [x]_\sim | \, x \in X \} .$$

Proof Let G be a group. Let $\varphi : [X]_\sim \to G$. Note $F_X = \langle [X]_\sim \rangle$. Let $\tilde{\varphi} : F \to G$. Set $([x]_\sim)\tilde{\varphi} = ([x]_\sim)\varphi$ for all $x \in X$. Suppose $\tilde{\varphi}$ is a homomorphism. For $\tilde{\varphi}$ to be a homomorphism, we must have

$$\left(([x]_\sim)^{-1}\right) \tilde{\varphi} = (([x]_\sim)\varphi)^{-1},$$

for every $x \in X$. In addition,

$$\left([x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}]_\sim\right) \tilde{\varphi} = \left([x_1]_\sim^{\varepsilon_1}\right) \varphi \left([x_2]_\sim^{\varepsilon_2}\right) \varphi \cdots \left([x_n]_\sim^{\varepsilon_n}\right) \varphi.$$

Since every the image of every element of F_X under $\tilde{\varphi}$ had only one possibility, we have a unique extension of φ to a homomorphism.

Theorem 1.2.3 (Universal Property) *Suppose F is a group with a free basis X. Then*

$$F \cong F_X.$$

Proof Since F is a group with free basis X, then the map

$$\begin{aligned} \phi : X &\to F_X \\ x &\mapsto [x]_\sim, \end{aligned}$$

then there is a unique homomorphism $\tilde{\phi}$ that is an extension of ϕ. Consider also the map

$$\begin{aligned} \theta : F_X &\to F \\ [x]_\sim &\mapsto x \end{aligned}$$

Note that θ is well-defined as under *theta*, all pairs of an element of X and its inverse will cancel; that is theta returns the unique irreducible element of $[x]_\sim$. Moreover, θ extends to a homomorphism by

$$\left([x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}]_\sim\right) \tilde{\theta} = (([x_1]_\sim)\theta)^{\varepsilon_1}(([x_2]_\sim)\theta)^{\varepsilon_2} \cdots (([x_n]_\sim)\theta)^{\varepsilon_n}.$$

Note that as $\tilde{\theta}$ and $\tilde{\phi}$ are onto the generators of F and F_X respectively, they are surjective. Direct computation shows that

$$x\tilde{\phi}\tilde{\theta} = x, \qquad [x]_\sim\tilde{\theta}\tilde{\phi} = [x]_\sim,$$

for every $x \in X$. Therefore $\tilde{\phi}$ and $\tilde{\theta}$ are left inverses and hence injective.

1.3 Rank

Definition 1.3.1 Let G be a group. The *rank* of G, denoted $d(G)$, is defined by

$$d(G) = \min\{|S| \big| G = \langle S \rangle\}.$$

Theorem 1.3.2 *Let X and Y be sets. We have*

$$F_X \cong F_Y \iff |X| = |Y|.$$

Proof ($\Rightarrow$): For any group F with free basis T, there exists a map

$$d_T : T \to \bigoplus_T \mathbb{Z}_2,$$

mapping $t \in T$ to the element of $\bigoplus_T \mathbb{Z}_2$ with a 1 in position t and $0s$ elsewhere. By the universal property, d_T extends to a homomorphism

$$\tilde{d_T} : T \to \bigoplus_T \mathbb{Z}_2.$$

Observe that $\tilde{d_T}$ is surjective, as it is onto the set of generators of $\bigoplus_T \mathbb{Z}_2$. Moreover,

$$\ker(\tilde{d_T}) = \langle w^2 | w \in F \rangle.$$

Note that the group $\langle w^2 | w \in F \rangle$ is independent of the basis, and is called the *square subgroup*. Furthermore, observe that

$$\left| \bigoplus_T \mathbb{Z}_2 \right| = \begin{cases} |\mathcal{P}(T)| & T \text{ finite} \\ |T| & T \text{ infinite} \end{cases}. \tag{1.1}$$

By the First Isomorphism Theorem,

$$F \big/ \ker(\tilde{d_T}) \cong \bigoplus_T \mathbb{Z}_2.$$

In particular, for two sets X and Y such that $F_X \cong F_Y$, we have that

$$F_X \big/ \ker(\tilde{d_X}) \cong F_Y \big/ \ker(\tilde{d_Y}).$$

However, we know that the above quotients groups have the same cardinality, therefore using 1.1 we conclude that

$$|X| = |Y|.$$

($\Leftarrow$): Let X and Y be sets such that $|X| = |Y|$. There is a bijection, say ϕ from X to Y. This induces a bijection from $[X]_\sim$ to $[Y]_\sim$. Since we have a function defined on the generators, this extends to a homomorphsim from F_X to F_Y, and back, since it is a bijection. Hence $F_X \cong F_Y$.

Corollary 1.3.3 *All free bases for a free group have the same cardinality.*

Definition 1.3.4 The free group with free basis of cardinality $n \in \mathbb{N}_0$ will be denoted F_n.

Theorem 1.3.5 *Let $m, n \in \mathbb{N}$ such that $m \geq n > 1$. Then*

$$F_n \hookrightarrow F_m \text{ and } F_m \hookrightarrow F_n.$$

Proof We have that $F_n \leq F_m$ so clearly $F_n \hookrightarrow F_m$.

Consider a map to a subset of a free basis of F_m of cardinality n to show $F_m \hookrightarrow F_n$. Suppose now that F_n and F_m have free bases

$$X_n = \{x_1,\ x_2, \dots,\ x_n\}, \quad X_m = \{y_1,\ y_2, \dots,\ y_m\},$$

respectively. Let

$$\begin{aligned} \phi : X_n &\to F_m \\ x_i &\mapsto {y_1}^{{y_2}^i} \end{aligned}$$

Let

$$u = y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}, \quad v = y_1^{\delta_1} \cdots y_n^{\delta_n},$$

with $\epsilon_i,\ \delta_i \in \{-1,\ 0,\ 1\}$ for all valid indices i. We have

$$u\tilde{\phi} = v\tilde{\phi} \implies (y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_m})\,\tilde{\phi} = \left(y_1^{\delta_1} \cdots y_n^{\delta_m}\right)\tilde{\phi}$$

$$\implies (y_1\phi)^{\varepsilon_1} \cdots (y_n\phi)^{\varepsilon_n} = (y_1\phi)^{\delta_1} \cdots (y_n\phi)^{\delta_n}.$$

Hence $u = v$ and $\tilde{\phi}$ is injective, and therefore a monomorphism.

Theorem 1.3.6 (Nielsen-Schreier Theorem) *Every subgroup of a free group F is a free group. If a subgroup G has finite index m in F, then*

$$m(\operatorname{rank} F - 1) = \operatorname{rank} G - 1.$$

Chapter 2

Presentations

2.1 Normal Closure

Definition 2.1.1 Let G be a group and $S \subseteq G$. The *normal closure* of S inside G is the smallest normal subgroup of G containing S. That is

$$\bigcap_{S \subseteq N \trianglelefteq G} N.$$

Notation 2.1.2 Let G be a group and $S \subseteq G$. Define

$$\langle\langle S \rangle\rangle = \langle S^G \rangle.$$

Lemma 2.1.3 *Let G be a group and $S \subseteq G$. Then*

$$\langle\langle S \rangle\rangle = \bigcap_{S \subseteq N \trianglelefteq G} N.$$

2.2 Group Presentations

Definition 2.2.1 Let X be a set $R \subseteq W(X)$. Define the *(group) presentation* on X, with *relations* R, denoted $\langle X|R \rangle$, by

$$\langle X|R \rangle = {}^{F_X}\!/\!_{\langle\langle [R]_\sim \rangle\rangle}.$$

Example 2.2.2 Consider

$$G = \langle a,\ b | a^{-1}b^{-1}ab \rangle.$$

We have

$$1_G =_G a^{-1}b^{-1}ab \implies ab =_G ba,$$

so G is abelian.

Example 2.2.3 We have

$$\begin{aligned}
\mathbb{Z} &\cong F_1 \cong \langle a| \rangle \\
F_2 &\cong \langle a,\ b| \rangle \\
C_6 &\cong \mathbb{Z}_6 \cong \langle a,\ b | a^2,\ b^3,\ [a,\ b] \rangle
\end{aligned}$$

Example 2.2.4 We have

$$\begin{aligned} Q_8 &\cong \langle a,\ b,\ c \mid a^2b^{-2},\ a^2c^{-2},\ a^4,\ abc^{-1},\ bca^{-1},\ cab^{-1}\rangle \\ &= {}^{F_{\{a,\ b,\ c\}}}\!\big/\!\langle\langle a^2b^{-2},\ a^2c^{-2},\ a^4,\ abc^{-1},\ bca^{-1},\ cab^{-1}\rangle\rangle \end{aligned}$$

2.3 Cayley Graphs

Definition 2.3.1 A *(multi)digraph* or a *(multiple) directed graph* G is a tuple $(V,\ E,\ s,\ t)$, where V is a set called the *vertices* of G and denoted $V(G)$ or G^0, E is a set called the *edges* of G and denoted $E(G)$ or G^1, and s and t are functions

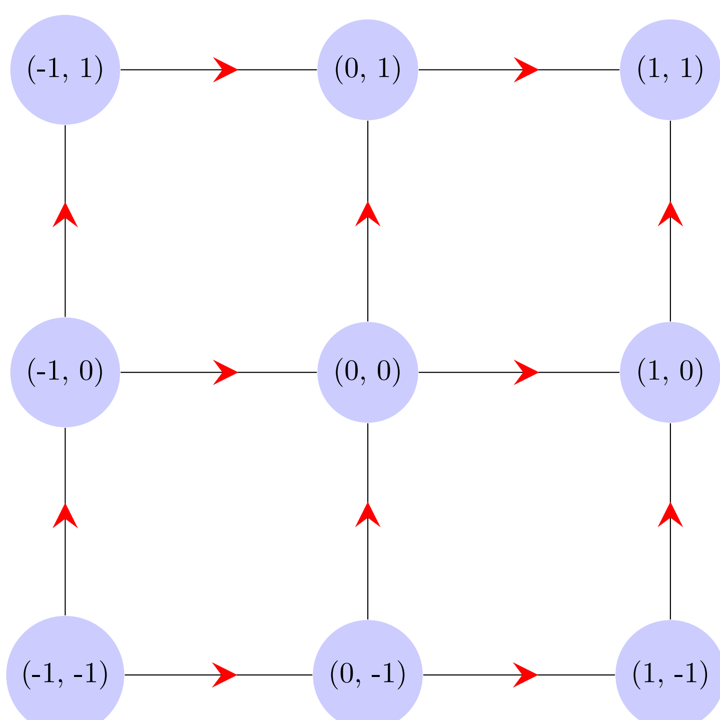
$$s : E \to V, \qquad t : E \to V.$$

Here s is used to represent the *start* vertex of an edge and t the *terminal* vertex.

Definition 2.3.2 Let G be a group, generated by a set X. The *(right) Cayley graph*, with respect to X, denoted $\Gamma(G,\ X)$, is defined by

$$\begin{aligned} &V(\Gamma(G,\ X)) = G \quad \text{(as a set)} \\ &E(\Gamma(G,\ X)) = \{(g,\ gx) \mid g \in G,\ x \in X\} \end{aligned}$$

Example 2.3.3 Let $G = \langle a,\ b \mid [a,\ b]\rangle$. Note that every element of G has a unique coset representative of the form $a^m b^n$ for some $m,\ n \in \mathbb{Z}$. So we will write $(m,\ n)$ to represent $[a^m b^n] \in G$. Part of the Cayley graph of G is given below.



Any non-identity element can be represented as a path on this graph. Since repeating the same path will never return to the start vertex, we can conclude that G is torsion-free.

2.4 Rewriting Systems

Definition 2.4.1 Let X be a set and $R \subseteq W(X)$. A *rewriting system* or a set of *rewrite rules* for $\langle X|R\rangle$ is a set of ordered pairs of elements of $W(X)$.

Remark 2.4.2 A rewriting system S can be used to alter words in a set, by replacing a subword equal to the first part of an element of S, with the second part.

Definition 2.4.3 A rewriting system where finitely many substitutions are applied before an irreducible word is reached is called *terminating* or *Noetherian.*

Let X be a set and $R \subseteq W(X)$. A rewriting system S of $\langle X|R\rangle$ is *confluent* if for all $w \in W(X)$ and for all $f,\ g \in \langle S\rangle$ there exists $f',\ g' \in \langle S\rangle$ such that $wgg' = wff'$.

A rewriting system is *complete*, if it is terminating and confluent.

Definition 2.4.4 Let X be a set, and S be a set of rewrite rules for X. We call S *locally confluent*, if for all $w \in W(X)$, with two rewrite rules $e_1,\ e_2$ that can alter w to obtain w_1 and w_2, there is a word $z \in W(X)$, that can be obtained from w_1 and w_2 by applying a sequence of substitutions

Lemma 2.4.5 (Newman's Lemma) *A terminating and locally confluent rewriting system is complete.*

Definition 2.4.6 Let X be a set and $R \subseteq W(X)$. A *normal form* for a presentation is a unique representative vertex in $W(X)$ for each equivalence class in $\langle X|R\rangle$.

Theorem 2.4.7 *Let X be a set and $R \subseteq W(X)$. If S is a terminating and confluent rewriting system for $\langle X|R\rangle$, then there is a normal form for $\langle X|R\rangle$.*

Example 2.4.8 Let $G = \langle a,\ b \mid a^2,\ b^3,\ abab\rangle$. Define

$$R = \{a^2 \mapsto \varepsilon,\ b^3 \mapsto \varepsilon,\ a^{-1} \mapsto a,\ b^{-1} \mapsto b^2,\ ba \mapsto ab^2\}.$$

TODO finish

2.5 Von Dyck's Theorem

Definition 2.5.1 Let F and G be groups and X be a basis for F. Let $\theta : X \to G$ be any function. The *linear extension* of θ, denoted $\tilde{\theta}$ is defined by

$$\begin{gathered}\tilde{\theta} : F \to G \\ x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \mapsto (x_1\theta)^{\varepsilon_1} (x_2\theta)^{\varepsilon_2} \cdots (x_n\theta)^{\varepsilon_n},\end{gathered}$$

noting that any element of F can be written as $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$, for some $n \in \mathbb{N}_0,\ x_i \in X, \varepsilon_i \in \{-1,\ 1\}$, for all valid indices i.

Theorem 2.5.2 (Von Dyck's Theorem) *Let X be a set and $R \subseteq W(X)$. Let $H = \langle X|R\rangle$ and G be a group. The linear extension of a function $\theta : X \to G$ is a group homomorphism if and only if $r\tilde{\theta} = 1_G$ for all $r \in R$.*

Example 2.5.3 Let $G = \langle a,\ b \mid a^2,\ b^3,\ abab \rangle$. Let

$$\begin{aligned} \theta : \{a,\ b\} &\to S_3 \\ a &\mapsto (1\ 2) \\ b &\mapsto (1\ 2\ 3) \end{aligned}$$

Note

$$\begin{aligned} a^2\tilde{\theta} &= (1\ 2)^2 = () \\ b^3\tilde{\theta} &= (1\ 2\ 3)^3 = () \\ abab\tilde{\theta} &= ((1\ 2)(1\ 2\ 3))^2 = (1\ 3)^2 = () \end{aligned}$$

Hence by Von Dyck's Theorem (Theorem 2.5.2), we have that $\tilde{\theta}$ is a group homomorphism. Since θ is onto the generators of S_3 we have that $\tilde{\theta}$ is surjective. Noting also that $|S_3| = 6 = |G|$, we have that $\tilde{\theta}$ is a bijection, and hence $G \cong S_3$.

Theorem 2.5.4 *Let G be a group. A set $X \subseteq G$ is a basis for G if and only if for all groups H and functions $\theta : X \to H$, we have that if there is a group homomorphism $\phi : G \to H$ extending θ, it is unique.*

2.6 Tietze Transformations

Definition 2.6.1 Let X be a set and $R \subseteq W(X)$. A set $S \subseteq R$ comprises *extraneous relators* if $S \subseteq \langle\langle R \backslash S \rangle\rangle$. A set $Y \subseteq X$ comprises *extraneous generators* if $Y \subseteq \langle X \backslash Y \rangle$.

Definition 2.6.2 The *Tietze transformations* for a group presentation are defined as

- T1 Add a set of extraneous relators,
- T2 Remove a set of extraneous relators,
- T3 Add a set of extraneous generators (name group elements),
- T4 Remove a set of extraneous generators.

Remark 2.6.3 When removing generators, their appearance in any relations must also be altered to ensure the generator appears nowhere in the presentation.

Example 2.6.4

$$\begin{tikzcd}
& \langle a,\ b \mid a^2,\ b^3,\ abab \rangle \arrow[dl, bend right, "\mathrm{T3}"'] \arrow[dr, bend left, "\mathrm{T1}"] & \\
\langle a,\ b,\ c,\ d \mid a^2,\ b^3,\ abab,\ c^{-1}a,\ d^{-1}aba \rangle \arrow[ur, bend left, "\mathrm{T4}"] & & \langle a,\ b \mid a^2,\ b^3,\ b^6,\ a^6,\ (ab)^{12},\ abab \rangle \arrow[ul, bend right, "\mathrm{T2}"']
\end{tikzcd}$$

Example 2.6.5 Is $\langle a,\ b \mid a^2,\ b^3,\ abab\rangle \cong \langle a,\ b \mid a^2,\ (ab)^3,\ b^2\rangle$?

Solution

$$\begin{aligned}
\langle a,\ b \mid a^2,\ (ab)^3,\ b^2\rangle &\underset{\text{T3}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ (ab)^3,\ b^2,\ c^{-1}(ab)\rangle \\
&\underset{\text{T1}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ (ab)^3,\ b^2,\ c^{-1}(ab),\ c^3\rangle, \\
\text{since } c^{-1}ab = 1 \implies c = ab,\ (ab)^3 = 1 \implies c^3 = 1& \\
&\underset{\text{T2}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ b^2,\ c^{-1}(ab),\ c^3\rangle \\
\text{since } c^{-1}ab = 1 \implies c = ab,\ c^3 = 1 \implies (ab)^3 = 1& \\
&\underset{\text{T1}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ b^2,\ c^{-1}(ab),\ c^3,\ b^{-1}a^{-1}c\rangle \\
&\underset{\text{T2}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ b^2,\ c^3,\ b^{-1}a^{-1}c\rangle \\
\text{since } c^{-1}ab = 1 \implies b^{-1}a^{-1}c = 1& \\
&\underset{\text{T4}}{\mapsto} \langle a,\ c \mid a^2,\ (a^{-1}c)^2,\ c^3,\ (a^{-1}c)^{-1}a^{-1}c\rangle \\
&\underset{\text{T2}}{\mapsto} \langle a,\ c \mid a^2,\ (a^{-1}c)^2,\ c^3\rangle \\
\text{since } (a^{-1}c)^{-1}a^{-1}c = c^{-1}aa^{-1}c = 1,\ \text{by free cancellations}& \\
&\underset{\text{T1}}{\mapsto} \langle a,\ c \mid a^2,\ (a^{-1}c)^2,\ c^3,\ acac\rangle \\
\text{since } a^2 = 1 \implies a^{-1} = a \implies acac = a^{-1}ca^{-1}c = 1& \\
&\underset{\text{T2}}{\mapsto} \langle a,\ c \mid a^2,\ c^3,\ acac\rangle \\
\text{since } a^2 = 1 \implies a^{-1} = a \implies a^{-1}ca^{-1}c = acac = 1& \\
&\underset{\text{T3}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ c^3,\ acac,\ b^{-1}c\rangle \\
&\underset{\text{T1}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ c^3,\ acac,\ b^{-1}c,\ b^3\rangle \\
\text{since } b^{-1}c = 1 \implies b = c \implies b^3 = c^3 = 1& \\
&\underset{\text{T2}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ acac,\ b^{-1}c,\ b^3\rangle \\
\text{since } b^{-1}c = 1 \implies b = c \implies c^3 = b^3 = 1& \\
&\underset{\text{T1}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ acac,\ b^{-1}c,\ b^3,\ abab\rangle \\
\text{since } b^{-1}c = 1 \implies b = c \implies abab = acac = 1& \\
&\underset{\text{T2}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ b^{-1}c,\ b^3,\ abab\rangle \\
\text{since } b^{-1}c = 1 \implies b = c \implies acac = abab = 1& \\
&\underset{\text{T1}}{\mapsto} \langle a,\ b,\ c \mid a^2,\ b^{-1}c,\ b^3,\ abab,\ c^{-1}b\rangle \\
\text{since } b^{-1}c = 1 \implies b^{-1}c = 1& \\
&\underset{\text{T4}}{\mapsto} \langle a,\ b \mid a^2,\ b^{-1}b,\ b^3,\ abab,\ b^{-1}b\rangle \\
&= \langle a,\ b \mid a^2,\ b^{-1}b,\ b^3,\ abab\rangle \\
&\underset{\text{T2}}{\mapsto} \langle a,\ b \mid a^2,\ b^3,\ abab\rangle \\
\text{since } bb^{-1} = 1,\ \text{by free cancellations}&
\end{aligned}$$

Theorem 2.6.6 (Tietze's Theorem) *If two presentations are isomorphic, then there is a chain of Tietze transformations from one to the other.*
If, in addition, the presentations are finite, then there is a finite chain.

2.7 Markov Properties

Definition 2.7.1 A statement about a group is a *property*, if it is preserved under isomorphism.

Definition 2.7.2 A property $\mathcal{P}$ is a *Markov property* if

0. (It is preserved under isomorphism),
1. There exists a finitely presented group with $\mathcal{P}$,
2. There exists a finitely presented group K which cannot embed into any finitely presented group with $\mathcal{P}$.

Example 2.7.3 By definition, triviality is preserved under isomorphism. A finite presentation $\langle a \mid a\rangle$ exists for a trivial group. The finitely presented group $\langle b \mid \rangle$ cannot embed into any trivial group, since it has infinite order, and trivial groups have finite order. Hence triviality is a Markov property.

Cardinality is preserved under bijection, hence finiteness is preserved under isomorphism. Therefore, using the same arguments as above, finiteness is a Markov property.

Let G and H be isomorphic groups. Suppose G is abelian. Let $\phi : G \to H$ be an isomorphism. Let $a,\ b \in H$ and $c,\ d \in G$ such that $c = a\phi^{-1},\ d = b\phi^{-1}$. We have

$$ab = (c\phi)(d\phi) = (cd)\phi = (dc)\phi = (d\phi)(c\phi) = ba,$$

and hence abelianness is preserved under isomorphism. A finite presentation $\langle a \mid a\rangle$ exists for an abelian group. The group $\langle a,\ b|\rangle$ is finitely presented and non-abelian. Since abelianness is preserved under subgroups, this cannot embed into any abelian group. Hence abelianness is a Markov property.

Theorem 2.7.4 (Markov) *If $\mathcal{P}$ is a Markov property, then there does not exist an algorithm which can take as input any finite presentation and decide in finite time whether or not the presentation presents a group with property $\mathcal{P}$.*

Chapter 3

Graphs, Actions and Categories

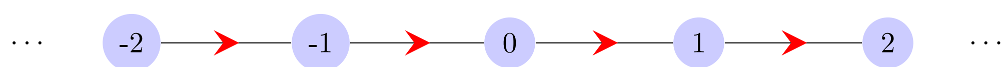
3.1 Graphs

Example 3.1.1 Let $L_{(\infty,\infty)} = (\mathbb{Z},\ E,\ s,\ t)$, where

$$E = \{(j,\ j+1) \mid j \in \mathbb{Z}\},$$

$$\begin{aligned} s : E &\to \mathbb{Z}, \\ (j,\ j+1) &\mapsto j \end{aligned} \qquad\qquad \begin{aligned} t : E &\to \mathbb{Z} \\ (j,\ j+1) &\mapsto j+1 \end{aligned}$$

This graph is called the *bi-infinite path*, and can be represented visually by



Definition 3.1.2 Let D be a digraph and $W \subseteq D^0$. The *induced subgraph* of D with vertex set W is the subgraph of D with vertex set W, edge set

$$\{e \in D^1 \mid s(e),\ t(e) \in W\},$$

and s and t functions defined by restricting the s and t functions of D to the new edge set.

Example 3.1.3 Let

$$\begin{aligned} V_{[0,n]} &= \{z \in \mathbb{Z} \mid z \in [0,n] \subseteq \mathbb{R}\} \\ V_{[0,\infty)} &= \{z \in \mathbb{Z} \mid z \in [0,\infty) \subseteq \mathbb{R}\} \\ V_{(-\infty,0)} &= \{z \in \mathbb{Z} \mid z \in (-\infty,0] \subseteq \mathbb{R}\} \end{aligned}$$

Define $L_{[0,n]}$ to be the induced subgraph of $L_{(-\infty,\infty)}$, with vertex set $V_{[0,n]}$, $L_{[0,\infty)}$, called the *right-infinite path*, to be the induced subgraph of $L_{(-\infty,\infty)}$, with vertex set $V_{[0,\infty)}$, and $L_{(-\infty,0]}$, called the *left-infinite path*, to be the induced subgraph of $L_{(-\infty,\infty)}$, with vertex set $V_{(-\infty,0]}$.

Definition 3.1.4 Let G and H be digraphs. A *graph homomorphsim* from G to H is a function

$$\phi : G^0 \sqcup G^1 \to H^0 \sqcup H^1,$$

such that for all $v \in G^0,\ v\phi \in H^0$, and for all $e \in G^1,\ e\phi \in H^1,\ es\phi = e\phi s$, and $et\phi = e\phi t$.

Definition 3.1.5 Let G be a digraph and $k \in \mathbb{N}_0$. A *path* in G of length k is a graph homomorphism from $L_{[0,k]}$ to G

Definition 3.1.6 A *simple graph* or *undirected graph* G is a tuple $(V,\ E,\ \text{ends})$, where V is a set called the *vertices* of G, E is a set called the *edges* of G and ends is a function

$$\begin{aligned} \text{ends} : E &\to \mathcal{P}(V) \\ e &\mapsto \{v_1,\ v_2\} \end{aligned}$$

Note in the above definition v_1 and v_2 need not be distinct. If e is an edge in G such that $\text{ends}(e) = \{v\}$ for some $v \in V$, then e is called a *loop*.

3.2 Categories

Definition 3.2.1 A *category* C is a tuple $(O,\ M,\ \circ)$, where O is a class called the *objects* of the category, denoted $\text{ob}(C)$. In addition, for each pair of objects in O, there is a collection of elements of M called morphisms. The set of morphisms is denoted $\text{hom}(C)$. Finally $\circ$ is defined as an associative binary operation on M, such that for each object a there is a morphism I_a from a to a, such that for any object b and morphism u from a to b and any morphism v from b to a we have $I_a \circ u = u$ and $v \circ I_a = v$.

A *functor* is a map from one category to another that preserves 'structure'.

Example 3.2.2 The class of groups forms a category with group homomorphisms as the morphisms. The class of digraphs forms a category with graph homomorphisms as the morphisms. The class of sets forms a category with functions as the morphisms. The class of topological spaces forms a category with continuous functions as the morphisms. The class of vector spaces over a field K is a category, with linear maps as the morphisms.

Example 3.2.3 There exists a functor $\mathscr{F}$ from the category of digraphs to the category of undirected graphs, which takes a digraph $(V,\ E,\ s,\ t)$ and maps it to an undirected graph G, with

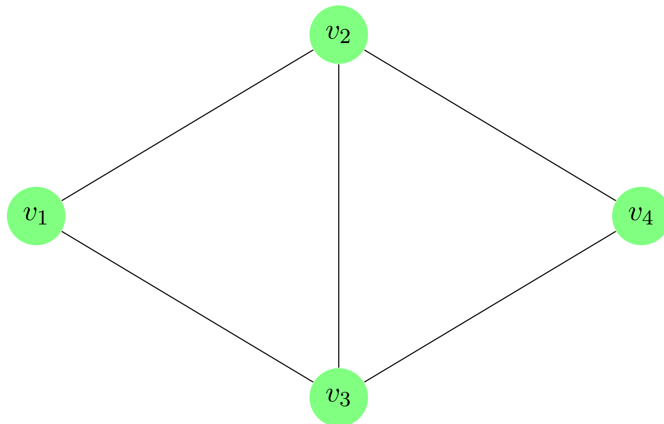
$$\begin{aligned} G^0 &= V \\ G^1 &= E \\ \text{ends} : G^1 &\to \mathcal{P}(G^1) \\ e &\mapsto \{es,\ et\} \end{aligned}$$

This functor is called the *forgetful functor*.

3.3 Group Actions

Definition 3.3.1 The *action* of a group G on a object O of a category is a group homomorphism $\varphi : G \to \text{Aut}(O)$. Action is often realised by elements of G appearing as functions of elements of O, whose images are the images of the automorphism the element of G maps to. If these functions are written to the right of elements of O, then G is said to have *right action* on O, denoted $O \curvearrowleft G$.

Example 3.3.2 Consider the undirected graph O:



Define a homomorphism from $\mathbb{Z}$ to $\mathrm{Aut}(O)$ as the linear extension of the homomorphism defined by $1 \mapsto (v_1\ v_4)(v_2\ v_3)$. This is the action of $\mathbb{Z}$ on O. Then

$$\begin{aligned} v_1 1 &= v_4 \\ v_3 1 &= v_2 \\ v_3 4 &= v_3 \end{aligned}$$

Definition 3.3.3 Let G be a group and X be a set such that $X \curvearrowleft G$. Let $k \in \mathbb{N}$. The action of G on X is

1. *faithful* if the group homomorphism from G to S_X has trivial kernel. That is, every non-trivial element of G moves some point in X,
2. *free* if every point in X is moved by every non-trivial element of G,
3. *transitive* if given $x,\ y \in X$, there exists $g \in G$ such that $xg = y$,
4. *k-transitive* if given any two k-tuples $(x_1,\ x_2,\ \dots,\ x_k)$, $(y_1,\ y_2,\ ,\dots,\ y_k) \in X^k$, then there is an element g of G, such that for all valid indices i, we have $x_i g = y_i$,
5. *regular* if the action of G on X is free and transitive,
6. *primitive* if the action of G on X is transitive, and it fails to preserve any non-trivial partition of X. That is, given a partition $\mathscr{P}$ of X, there is an element g of G and a set $U \in \mathscr{P}$, such that $Ug \notin \mathscr{P}$.

Theorem 3.3.4 *A group G acts on a set X if and only if there exists an operation*

$$\begin{aligned} \bullet : X \times G &\to X \\ (x,\ g) &\mapsto x \bullet g \end{aligned}$$

such that

1. *For all $x \in X,\ x \bullet 1_G = x$,*
2. *For all $x \in X$ and $g,\ h \in G,\ (x \bullet g) \bullet h = x \bullet (gh)$.*

Definition 3.3.5 Let G be a group and $H \leq G$. The *core* of H in G, denoted $\mathrm{Core}_G(H)$ is defined by

$$\mathrm{Core}_G(H) = \bigcap_{x \in G} x^{-1}Hx.$$

Theorem 3.3.6 (Cayley's Theorem) *Let $H \leq G$ for some group G. Let M be the set of right cosets of H in G. Define a mapping $\varphi : G \to S_M$ by the rule:*

for any $g \in G$ the permutation $g\varphi$ maps Hx to Hxg, where $x \in G$.

Then φ is a group homomorphism and

$$\ker\varphi = \mathrm{Core}_G(H).$$

Proof Let $G,\ H,\ M$ be defined as stated in the theorem. We will (1) show φ is a group homomorphism and (2) show $\ker\phi = \mathrm{Core}_G(H)$.

1. Let $x,\ g,\ h \in G$. Note that $g\varphi$ is a well-defined function of M, since it maps cosets to cosets. We have

$$\begin{aligned}((Hx \cdot (g\varphi)) \cdot (g^{-1}\varphi) &= (Hxg) \cdot (g^{-1}\varphi) \\ &= Hxgg^{-1} \\ &= Hx\end{aligned}$$

$$\begin{aligned}((Hx \cdot (g^{-1}\varphi)) \cdot (g\varphi) &= (Hxg^{-1}) \cdot (g\varphi) \\ &= Hxg^{-1}g \\ &= Hx,\end{aligned}$$

so $g^{-1}\varphi$ is the inverse of $g\varphi$ and hence $g\varphi$ is a permutation. In addition

$$Hx(g\varphi)(h\varphi) = (Hxg)(h\varphi) = H(xg)h = Hx(gh) = (Hx)((gh)\varphi),$$

and it follows that φ is a group homomorphism.

2. Let $k \in G$. Then

$$\begin{aligned}k \in \ker\varphi &\iff Hxkx^{-1} = H \quad \text{for all } x \in G \\ &\iff xkx^{-1} \in H \quad \text{for all } x \in G \\ &\iff k \in x^{-1}Hx \quad \text{for all } x \in G \\ &\iff k \in \bigcap_{x \in G} x^{-1}Hx.\end{aligned}$$

Hence

$$\ker\varphi = \bigcap_{x \in G} x^{-1}Hx.$$

Corollary 3.3.7 *Let G be a group. Then*

1. *There exists an embedding of G into S_G,*

2. *Suppose $|G| = n$ for some $n \in \mathbb{N}$. It is possible to embed G into $\mathrm{GL}_n(R)$, where R is any ring.*

Proof Part 1 follows easily. Consider that any permutation group of size n, where $n \in \mathbb{N}$, can be realised as a group of permutations of the canonical base vectors $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$. The matrices for these permutations will have the property that each row and column have precisely one 1, and the remainder of the entries are zeros. Such a matrix will have determinant ± 1.

Corollary 3.3.8 (Poincaré) *Let G be a group. Every subgroup H of finite index $m \in \mathbb{N}$, contains a normal subgroup N of G which has finite index $k \in \mathbb{N}$ in G such that*

$$m|k, \qquad k|m!.$$

Proof Let G be a group and $H \leq G$ such that $[G : H] = m$, where $m \in \mathbb{N}$. Let φ be defined as in Cayley's Theorem (Theorem 3.3.6). Let $Q = {}^{G}\!/_{\ker\varphi}$, where here we will use right cosets. We have have that $ker\varphi \trianglelefteq G$. Since there are m cosets of H in G, we have that Q embeds in S_m. Let $k = |Q|$. Note $k = [G : \ker\varphi]$. The cosets of $\ker\varphi$ are the elements of Q, so by Lagrange's Theorem $k = |Q|\big|m!$. The image of H under φ is a subgroup of Q with index m, by the Correspondence Theorem, noting that $\ker\varphi \leq H$. Hence, by Lagrange's Theorem, $m|k$.

Corollary 3.3.9 *Infinite simple groups have no proper finite index subgroups.*

Proof Suppose G is an infinite simple group. Suppose G has a subgroup H of finite index m. Then, by Corollary 3.3.8, there is a normal subgroup N of G with finite index k, such that $k|m$ and $m|k$. Since N is normal and k is finite, we have that $k = 1$. It follows that $m = 1$, and hence $H = G$.

3.4 Orbits and Stabilisers

Definition 3.4.1 Let G be a group and X be a set such that $X \curvearrowleft G$. Let $x \in X$. The *orbit* of x under the action of G, denoted $\mathscr{O}_G(x)$ or xG, is defined by

$$\mathscr{O}_G(x) = \{xg \mid g \in G\}.$$

Lemma 3.4.2 *Let G be a group and X be a set such that $X \curvearrowleft G$. The orbits of X under G partition X.*

Proof Let G, X by defined as in the statement of the Lemma. Let x, $y \in X$ such that $xG \cap yG \neq \emptyset$. Then there are elements g, $h \in G$ such that $xg = yh$. Let $k \in G$ be arbitrary. Then $xk = xgg^{-1}k = yhg^{-1}k \in yG$ and hence $yG \subseteq xG$. By symmetry $xG \subseteq yG$ and $xG = yG$. So orbits are disjoint or equal, and hence they partition X.

Definition 3.4.3 Let G be a group and X be a set such that $X \curvearrowleft G$. Let $Y \subseteq X$. The *stabiliser* of Y under the action of G, denoted $\mathrm{Stab}_G(Y)$ is defined by

$$\mathrm{Stab}_G(Y) = \{g \in G \mid Yg = Y\}.$$

If $Y = \{y\}$ for some $y \in X$, then the stabiliser of Y is called the *point stabiliser* of y, and is denoted $\mathrm{Stab}_G(y)$ or G_y.

Lemma 3.4.4 *Let G be a group and X be a set such that $X \curvearrowleft G$. Let $Y \subseteq X$. Then $\mathrm{Stab}_G(Y) \leq G$.*

Proof Let $G,\ X,\ Y$ be defined as in the statement of the theorem. Let $g,\ h \in \mathrm{Stab}_G(Y)$. We have $Ygh = Yh = Y$, hence $gh \in \mathrm{Stab}_G(Y)$. In addition, $Y = Y1_G = Ygg^{-1} = Yg^{-1}$, and hence $g^{-1} \in \mathrm{Stab}_G(Y)$. We can conclude that $\mathrm{Stab}_G(Y) \leq G$.

Theorem 3.4.5 (Orbit-Stabiliser Theorem) *Let G be a group and X be a set such that $X \curvearrowleft G$. If $x \in X$ then*

$$|xG| = [G : G_x].$$

If, in addition, G is finite, then

$$|G| = |xG||G_x|.$$

In particular, the orders of the orbit and point stabiliser of x divides the order of the group.

Proof Let $G,\ X,\ x$ be defined as stated in the theorem. Let M denote the set of right cosets of G_x in G. Define

$$\begin{aligned} \theta : xG &\to M \\ xg &\mapsto G_x g \end{aligned}$$

Let $g,\ h \in G_x$. Then $xgh^{-1} \in G_x$ and hence

$$xg\theta = G_x g = G_x h = xh\theta,$$

and θ is well-defined. If $xg\theta = xh\theta$ then $G_x g = G_x h$, which implies $G_x gh^{-1} = G_x$. It follows that $xgh^{-1} = x$ and hence $xg = xh$, so θ is injective. Finally, if $G_x k$ is a coset of G, then the point $xk \in xG$ is sent to $G_x k$ by θ, and hence θ is surjective, and therefore a bijection. It follows that $|xG| = |M| = [G : G_x]$. The other statements of the theorem follow by Lagrange's Theorem.

3.5 Normalisers and Centralisers

Lemma 3.5.1 *A groups acts on itself by conjugation.*

Proof Let G be a group. For $g \in G$, define

$$\begin{aligned} \varphi_g : G &\to G \\ h &\mapsto h^g \\ \psi_g : G &\to G \\ h &\mapsto h^{g^{-1}} \end{aligned}$$

Let $g,\ h \in G$. We have

$$\begin{aligned} h\psi_g\varphi_g &= ghg^{-1}\varphi_g g^{-1}ghgg^{-1} = h, \\ h\varphi_g\psi_g &= g^{-1}hg\psi_g gg^{-1}hg^{-1}g = h, \end{aligned}$$

and hence ψ_g and φ_g are each others inverses, and it follows that φ_g is a bijection.

Let $g,\ h,\ k \in G$. We have

$$(hk)\varphi_g = g^{-1}hkg = g^{-1}hgg^{-1}kg = h\varphi_g k\varphi_g,$$

and hence φ_g is a group homomorphism. We can conclude that for all $g \in G,\ \varphi_g$ is an automorphism of G.

Define

$$\begin{aligned} \phi : G &\to \mathrm{Aut}(G) \\ g &\mapsto \varphi_g \end{aligned}$$

Let $g,\ h,\ k \in G$. We have

$$k((gh)\phi) = k\varphi_{gh} = (gh)^{-1}kgh = h^{-1}g^{-1}kgh = g^{-1}kg\varphi_h = k\varphi_g\varphi_h = k((g\phi)(h\phi)),$$

and hence ϕ is a group homomorphism, and G acts on itself by conjugation.

Definition 3.5.2 Let G be a group, acting on itself by conjugation. Let $S \subseteq G$. The *normaliser* of S in G, denoted $N_G(S)$, is defined by

$$N_G(S) = \{g \in G \mid S^g = S\}.$$

The *centraliser* of S in G, denoted $C_S(G)$, is defined by

$$C_G(S) = \{g \in G \mid s^g = s,\ \forall s \in S\}.$$

Lemma 3.5.3 *Let G be a group and $S \subseteq G$. Then*

$$Z(G) = C_G(G).$$

Proof Let $g \in G$. Then

$$\begin{aligned} g \in Z(G) &\iff gh = hg,\ \forall h \in G \\ &\iff h = g^{-1}hg, \forall h \in G \\ &\iff g \in C_G(G) \end{aligned}$$

Lemma 3.5.4 *Let G be a group. If $S,\ T \subseteq G$ then*

$$S \subseteq C_G(T) \iff T \subseteq C_G(S).$$

Proof Let G be a group and $S,\ T \subseteq G$.
($\Rightarrow$): Suppose $S \subseteq C_G(T)$. Let $s \in S$ and $t \in T$. We have

$$s^{-1}ts = t \implies ts = st \implies t^{-1}tst = s \implies t \in C_G(S),$$

and hence T $\subseteq C_G(S)$.

($\Leftarrow$): The converse follows by symmetry of S and T.

Lemma 3.5.5 *The relation of elements of a group being conjugate is an equivalence relation*

Proof Let G be a group and $g,\ h,\ k \in G$. Use the symbol $\sim$ to denote the relation. Reflexivity: $g = 1_G^{-1}g1_G$, so $g \sim g$. Symmetry: if $g \sim h$ then there exists $a \in G$ such that $g = a^{-1}ha$. Hence $h = aga^{-1} = g^{a^{-1}}$ and $h \sim g$. Transitivity: if $g \sim h$ and $h \sim k$ then there exist $a,\ b \in G$ such that $g = a^{-1}ha$ and $h = b^{-1}kb$. Then $g = a^{-1}b^{-1}kba = (ba)^{-1}k(ba)$ and so $g \sim k$.

Definition 3.5.6 The equivalence classes of a group, under the equivalence relation of conjugacy, are called the *conjugacy classes* of the group.

Lemma 3.5.7 *An element x of a group G is the only conjugate of itself if and only if $x \in Z(G)$.*

Proof Let G be a group and $x \in G$. The only conjugate of x is x if and only if, for all $g \in G$ we have that $g^{-1}xg = x$. This is true if and only if $xg = gx$, which is the definition of x being in the centre.

Theorem 3.5.8 (The Class Equation) *Let G be a group and Γ be the set of conjugacy classes of G, not including $Z(G)$. For each $X \in \Gamma$, let $x_X \in X$ be arbitrary. Then*

$$|G| = |Z(G)| + \sum_{X \in \Gamma} [G : C_G(x_X)].$$

Proof Let G and Γ be defined as in the theorem. Consider the conjugacy class of an element of G as the orbit under the action of G on itself by conjugation. We have from Lemma 3.5.7, that the orbits of elements of the centre have size 1. By the Orbit-Stabiliser Theorem (Theorem 3.4.5), we have that the size of the orbit of an arbitrary element x is equal to the index of the point stabiliser in G.We have that the point stabiliser of an element x is

$$\{g \in G \mid x^g = x\} = C_G(x).$$

Since the conjugacy classes partition G, summing them gives the class equation.

Chapter 4

Formal Language Theory

4.1 Recognisable and Rational Languages

Definition 4.1.1 Let Σ be a finite set. We will refer to Σ as an *alphabet*, and the elements of Σ as *letters* or *symbols*. A subset $L \subseteq \Sigma^*$ is a called a *language* over Σ.

Definition 4.1.2 Let M and N be monoids, where N is finite. A subset $L \subseteq M$ is called *recognisable* if there exists a monoid homomorphism $\tau : M \to N$ such that $(L\tau)\tau^{-1} = L$. Note that here, $\tau{-1}$ is used to denote the pre-image.

Definition 4.1.3 Let M and H be groups, where H is finite. A subset $L \subseteq G$ is called *recognisable* if there exists a group homomorphism $\tau : M \to N$ such that $(L\tau)\tau^{-1} = L$. Note that here, τ^{-1} is used to denote the pre-image.

Definition 4.1.4 Let M be a monoid. The set $\mathrm{Rat}(M)$ of *rational* subsets of M is defined inductively as follows:

1. Finite subsets of M are rational,
2. If $K,\ L \in \mathrm{Rat}(M)$, then $K \cup L \in \mathrm{Rat}(M)$,
3. If $K,\ L \in \mathrm{Rat}(M)$, then $KL = \{kl \mid k \in K,\ l \in L\} \in \mathrm{Rat}(M)$,
4. If $L \in \mathrm{Rat}(M)$, then $L^* \in \mathrm{Rat}(M)$.

Example 4.1.5 Let $\Sigma = \{0,\ 1,\ 2\}$. Let $w_1,\ w_2,\ w_3 \in \Sigma^*$. Observe that the expression

$$\{0\} \cup \{0112\} \cup \{w_1\}^*\{w_2\}\{0\} \cup \{w_2\}\{w_1\}\{w_3,\ 01\}^*\{w_1\},$$

is a rational subset of Σ^*. Note here Σ^* is a monoid under concatenation of words.

4.2 Regular Languages

Definition 4.2.1 A tuple $\mathcal{A} = (Q,\ \Sigma,\ \delta,\ I,\ F)$ is a *finite state automaton* if

1. The symbol Q denotes a finite set. Here Q is referred to as the *states* of $\mathcal{A}$,
2. The symbol Σ denotes a finite set. Here Σ is referred to as the *alphabet* of $\mathcal{A}$,

3. The symbol δ denotes a subset of $(Q \times \Sigma) \times Q$. This is called the *transition relation* of $\mathcal{A}$,

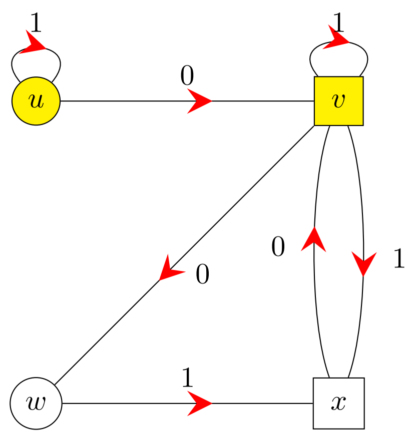
4. The symbol I denotes a subset of Q. This is referred to as the set of *initial states* or *start states* of $\mathcal{A}$,

5. The symbol F denotes a subset of Q. This is referred to as the set of *terminal states* or *accept states* of $\mathcal{A}$.

Example 4.2.2 Let $Q = \{u,\ v,\ w,\ x\},\ \Sigma = \{0,\ 1\},\ I = \{u,\ v\}, F = \{v,\ x\}$, and

$$\delta = \{((u,\ 1),\ u),\ ((u,\ 0),\ v),\ ((v,\ 1),\ v),\ ((v,\ 1),\ x),\ ((v,\ 0),\ w)\ ((x,\ 0),\ v), ((w,\ 1),\ x)\}.$$

Then $\mathcal{A} = (Q,\ \Sigma,\ \delta,\ I,\ F)$ is a finite state automaton and can be represented graphically as:



Here the start states are coloured yellow, and the end states are squares.

Definition 4.2.3 For every finite state automaton $\mathcal{A}$, there is a language determined by $\mathcal{A}$, denoted $L(\mathcal{A})$, defined as the set of all words $w \in \Sigma^*$, such that there is a path starting at a start state, ending at a terminal state, and the labels of the path, when concatenated, equal w.

If L is a language and $L = L(\mathcal{A})$ for some automaton $\mathcal{A}$ then L is *accepted* by $\mathcal{A}$.

Example 4.2.4 Let $\mathcal{A}$ be defined as in Example 4.2.2. Then

$$0,\ 111101111, 001 \in L(\mathcal{A}).$$

Definition 4.2.5 A finite state automaton $\mathcal{A} = (Q,\ \Sigma,\ \delta,\ I,\ F)$ is *deterministic* if, given $v \in Q$ and $x \in \Sigma$, there is a unique $u \in Q$, such that $((v,\ x),\ u) \in \delta$. If $\mathcal{A}$ is not deterministic, then $\mathcal{A}$ is called *non-deterministic*.

Theorem 4.2.6 (Kleene's Theorem) *Let Σ^* be a finitely generated free monoid, over a set Σ. Let $L \subseteq \Sigma^*$ be a language. Then the following are equivalent:*

1. *The language L is recognisable,*

2. *The language L is accepted by some deterministic finite state automaton,*

3. *The language L is accepted by some non-deterministic finite state automaton,*

4. The language L is rational.

Proof (1) $\implies$ (2): Suppose L is recognisable. Then there is a finite monoid N, and a monoid homomorphism $\tau : \Sigma^* \to N$, such that $(L\tau)\tau^{-1} = L$. Let

$$\mathcal{A} = (L,\ \Sigma,\ \delta,\ \{1_N\},\ L\tau),$$

where $\delta = \{((n,\ a),\ n(a\tau)) \mid n \in N,\ a \in \Sigma\}$. By the definition of δ, given $a \in \Sigma$ and $n \in N$, we have precisely one transition relation, so $\mathcal{A}$ is a deterministic finite state automaton.

Let $w = a_1 a_2 \cdots a_k \in \Sigma^*$, for some $k \in \mathbb{N}_0$, where $a_i \in \Sigma$, for all valid i. Let p be the state reached after reading w in $\mathcal{A}$. For each letter a_i in w that we read, we move from state n, to state $n(a_i\tau)$. Hence reading w, using the fact that τ is a monoid homomorphism, gives

$$(((1_N(a_1\tau))(a_2\tau)) \cdots (a_k\tau)) = (a_1 a_2 \cdots a_k)\tau.$$

We have that $(a_1 a_2 \cdots a_k)\tau \in L\tau$ if $w \in L$, so $L \subseteq \mathscr{L}(\mathcal{A})$. In addition, if w is accepted by $\mathcal{A}$, then $(a_1 a_2 \cdots a_k)\tau \in L\tau$, and hence $(w \in L\tau$. Since $(L\tau)\tau^{-1} = L$, we have that $w\tau\tau^{-1} \in L$, and hence $\mathscr{L}(\mathcal{A}) \subseteq L$.

(2) $\implies$ (3): Let $\mathcal{A}$ be a deterministic finite state automaton accepting L. Let q be a terminal state of $\mathcal{A}$. Create a new automaton $\mathcal{B}$, with all states and relations as $\mathcal{A}$, and an additional terminal state q', and for each relation in $\mathcal{A}$ that has q is its second part, there is a relation in $\mathcal{B}$ with q' as its second part, and the same first part. We have that $\mathcal{B}$ is non-deterministic, and accepts the same language as $\mathcal{A}$, which is L.

(3) $\implies$ (4): Let $\mathcal{A}$ be a finite state automaton accepting L. Let n be the number of states in $\mathcal{A}$, and we will refer to these states as $a_1,\ \ldots,\ a_k$. For all $i,\ j,\ k \in \{1,\ \ldots,\ n\}$, define $J^k_{i,j}$ to be the language comprising all words that when read in $\mathcal{A}$, starting at a_i, terminate at a_j, without passing through a_m, for any $m \in \mathbb{N},\ m > k$, excepting the start and finish of the path, even if i or j are greater than k. Note that $J^0_{i,j}$ comprises all letters a such that $((a_i,\ a), a_j)$ is a transition relation of $\mathcal{A}$, and if $i = j$, then $\varepsilon \in J^0_{i,\ j}$. Note that as $J^0_{i,j}$ is finite, since Σ is finite, for any valid i and j, we have that it is rational. Inductively suppose $J^k_{i,j}$ is rational, for some k. Then

$$J^k_{i,j} = J^{k-1}_{i,j} \cup J^{k-1}_{i,k} \cdot \left(\bigcup_{p \leq k} J^p_{k,k} \right)^* \cdot J^{k-1}_{k,j}. \tag{4.1}$$

Hence $J^k_{i,j}$ is also rational, as it is constructed using rational sets and the rational definition. We can conclude that for all $i,\ j,\ k \in \{1, \ldots,\ n\}$, we have that $J^k_{i,j}$ is rational. Let I and F be the initial and terminal states of $\mathcal{A}$, For $i,\ j,\ k \in \{1,\ \ldots,\ n\}$, define

$$L^k_{i,j} = \begin{cases} J^k_{i,j} & a_i \in I,\ a_j \in F \\ \emptyset & \text{otherwise} \end{cases}.$$

Since $J^k_{i,j}$ is rational for all valid $i,\ j$ and k, and, as a finite set, the empty set is rational, we have that $L^k_{i,j}$ is rational. In addition

$$L = \mathscr{L}(\mathcal{A}) = \bigcup_{i,j,k} L^k_{i,j}.$$

As a finite union of rational sets, L is rational.

(4) $\implies$ (1):

Definition 4.2.7 Any language satisfying any of the conditions of Kleene's Theorem (Theorem 4.2.6) is called *regular*.

Theorem 4.2.8 (Pumping Lemma for Regular Languages) *Let L be a regular language over a finite alphabet Σ. Then there exists $N \in \mathbb{N}$, such that if $w \in L$ satisfies $|w| > N$, then there are words $x,\ y,\ z \in \Sigma^*$, such that $|y| > 0$, and for all $n \in \mathbb{N}_0$,*

$$xy^n z \in L.$$

Proof Let $\mathcal{A}$ be a deterministic finite state automaton for L, and let $N \in \mathbb{N}$ be the number of states of $\mathbb{A}$. Suppose $w \in L$ has length greater than N. When w is read in $\mathcal{A}$, there exists a state q, that is visited at least twice. Let y be the subword of w that is read to get from the first visitation of q to the second, when reading w in $\mathcal{A}$. Let $x,\ z \in \Sigma^*$ be the prefix and suffix of w, such that $w = xyz$. Since y takes q to itself, the word $xz = xy^0z$ will take a start state to a terminal state. In addition, repeating y will also take q to itself. Hence xy^nz is accepted by $\mathcal{A}$, for all $n \in \mathbb{N}$, and hence is in L.

4.3 Anisimov's Theorem

Definition 4.3.1 Let G be a group, generated by a finite set X. We define the *word problem* in G with respect to X, denoted $\mathrm{WP}(G,\ X)$, by

Example 4.3.2 Let $G = \langle a,\ b \mid [a,\ b]\rangle$. Then

$$\begin{aligned}\mathrm{WP}(G,\ X) &= \{w \in W(\{a,\ b\}) \mid w =_G 1_G\} \\ &= \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \mid n \in \mathbb{N}_0,\ x_i \in \{a,\ b\},\ \varepsilon_i \in \{-1,\ 1\} \text{ for all valid } i, \text{ such that} \\ &\qquad \sum_{x_i=a} \varepsilon_i = \sum_{x_i=b} \varepsilon_i = 0\}\end{aligned}$$

For example,

$$a^{-1}bba^{-1}b^{-1}ab^{-1}a \in \mathrm{WP}(G,\ X).$$

Theorem 4.3.3 (Anisimov's Theorem) *Let G be a group generated by a finite set X. Then G is finite if and only if $\mathrm{WP}(G,\ X)$ is a regular language over $X \cup X^{-1}$.*

Proof ($\Rightarrow$): Suppose G is a finite group with generating set X. Consider the Cayley graph $\Gamma(G,\ X \cup X^{-1})$ as a deterministic automaton $\mathcal{A}$, with initial and final states being $\{1_G\}$. If $w \in \mathrm{WP}(G,\ X)$, then the word traced by w in the automaton, starting at 1_G, will end at 1_G, so $w \in L(\mathcal{A})$ and $\mathrm{WP}(G,\ X) \subseteq L(\mathcal{A})$. Any word in $L(\mathcal{A})$ will trace a path from 1_G to itself, and so will be in $\mathrm{WP}(G,\ X)$, and we can conclude $\mathrm{WP}(G,\ X)$ is a regular language.

($\Leftarrow$): Suppose $\mathrm{WP}(G,\ X)$ is a regular language over $X \cup X^{-1}$. Suppose, for contradiction, that G is infinite. Then there exists an infinite family of words $(w_i)_{i\in\mathbb{N}} \subseteq W(X)$, where $|w_i| \to \infty$, and given any $i \in \mathbb{N}$, no proper substring of w_i represents the trivial word. This is true, because if it fails, then there is a $n \in \mathbb{N}$, such that every word of length greater than n is equivalent in G to something shorter, which implies G is finite.

Let $\mathcal{A}$ be the automaton accepting $\mathrm{WP}(G,\ X)$. We will use the powerset construction of $\mathcal{A}$, to assume $\mathcal{A}$ is deterministic, has a unique start state and a has a unique accept state.

Claim: There exists some $m \in \mathbb{N}$, such that w_m has two distinct proper prefixes, u and uv, such that when reading u or uv from the start state of $\mathcal{A}$ to itself.

If the claim were false, then $\mathcal{A}$ would be infinite, since $|w_m| \to \infty$, a contradiction. That is, if $q = |Q_A|$, then there exists some $m \in \mathbb{N}$, such that $|w_m| > |Q_A|$, and hence any subword of $|w_m|$ of length $q+1$, must visit some state twice.

It follows from the claim that $uvu^{-1} \in \mathrm{WP}(G,\ X)$, because $uu^{-1} =_G 1_G$, and reading uu^{-1} and uvu^{-1}, will take us to the same state. Hence $uvu^{-1} =_G 1_G$, and we can conclude $v =_G 1_G$. But no proper substring of w_i is trivial, a contradiction.

4.4 Context Free Languages

Definition 4.4.1 A *context free grammar* g is a four-tuple

$$g = (V,\ \Sigma,\ P,\ s),$$

where V is a finite set of *non-terminal symbols*, Σ is a finite set, disjoint from V, of *terminal symbols* (or *letters*), $P \subseteq V \times (V \cup \Sigma)^*$ is a finite relation, called the *productions*, and $s \in V$ is called the *start symbol.*

The *language* of g, denoted $\mathscr{L}(g)$, is defined as the set of elements of Σ^* that are the result of a sequence of productions starting from s.

Let Σ be any alphabet. A language $L \subseteq \Sigma^*$ is called *context free*, if there is a context free grammar g, such that $L = \mathscr{L}(g)$.

Remark 4.4.2 It is possible to view productions of a context free grammar, as a set of rewrite rules.

Example 4.4.3 Let

$$g = (\{s\},\ \{a\},\ P,\ s),\ \tilde{g} = (\{s\},\ \{a\},\ \tilde{P},\ s),$$

where $P = \{(s,\ sa),\ (s,\ a)\}$ and $\tilde{P} = \{(s,\ sa),\ (s,\ \varepsilon)\}$. Then

$$\mathscr{L}(g) = \{a^k \mid k \in \mathbb{N}\}, \quad \mathscr{L}(\tilde{g}) = \{a^k \mid k \in \mathbb{N}_0\}.$$

Definition 4.4.4 A seven-tuple $\mathcal{A} = (Q,\ \Sigma,\ \chi,\ \delta,\ q_0,\ \perp,\ F)$ is a *pushdown automaton*, if

1. Q is a finite set, called the set of *states*,
2. Σ is a finite set, called the *alphabet*,
3. χ is a finite set, called the *stack alphabet*,

4. $\delta \subseteq (Q \times (\Sigma \cup \{\varepsilon\}) \times \chi^*) \times (Q \times \chi^*)$ is called the *transition relation*,
5. $q_0 \in Q$ is called the *start state*,
6. $\perp \in \chi$ is called the *bottom of stack symbol*,
7. $F \subseteq Q$ is called the set of *accept states*.

The *language* of $\mathcal{A}$, denoted $\mathscr{L}(\mathcal{A})$, is defined as the set of words over Σ, that when applied into the transition relation, starting at q_0, end at an accept state.

Remark 4.4.5 Pushdown automata have the following 'idea':

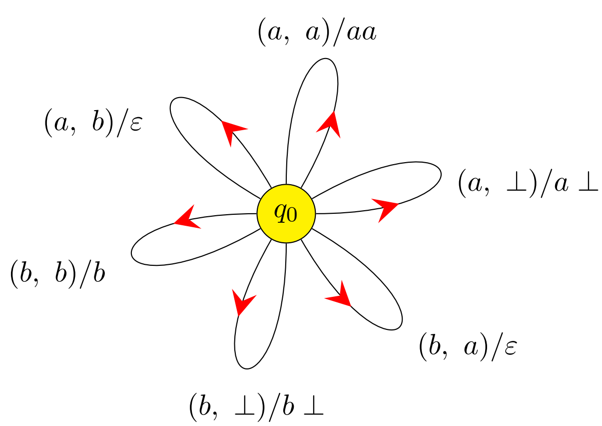
1. Read an input tape $w \in \Sigma^*$,
2. Read the next letter u from the input tape (or word). Read a 'small' word v on the top of the stack. Notice current state $x \in Q$ (start at the start state q_0,
3. Move to new state $y \in Q$, and change v to $\tilde{v} \in \chi^*$, where $((x,\ u,\ v),\ (y,\ \tilde{v}))$,
4. When finished reading the input tape, if the active state is in F, then w is accepted.

Note that with this 'accept rule', $\perp$ is irrelevant, but there are 'accept rules', which require $\perp$.

Example 4.4.6 Let $Q = \{q_0\},\ \Sigma = \{a,\ b\},\ \chi = \{a,\ b,\ \perp\}$ and $F = \{q_0\}$. Let

$$\begin{aligned}\delta = \{&((q_0,\ a,\ \perp),\ (q_0,\ a\perp)),\ ((q_0,\ a,\ a),\ (q_0,\ aa)),\ ((q_0,\ a,\ b),\ (q_0,\ \varepsilon)),\\ &((q_0,\ b,\ \perp),\ (q_0,\ b\perp)),\ ((q_0,\ b,\ b),\ (q_0,\ bb)),\ ((q_0,\ b,\ a),\ (q_0,\ ba))\}\end{aligned}$$

Let $\mathcal{A} = (Q,\ \Sigma,\ \chi,\ \delta,\ q_0,\ \perp,\ F)$. We have that $\mathscr{L}(\mathcal{A}) = \Sigma^*$. Note that $\mathcal{A}$ can be represented graphically by



Theorem 4.4.7 *Let Σ be a finite alphabet and $L \subseteq \Sigma^*$ be a language. Then the following are equivalent:*

1. *The language L is context-free,*

2. *The language L is accepted by a deterministic pushdown automaton,*

3. *The language L is accepted by a non-deterministic pushdown automaton.*

Proof (2) $\implies$ (3): Adding redundant transitions to a deterministic pushdown automaton creates a non-deterministic one.

(3) $\implies$ (1): Let L be the language accepted by a pushdown automaton $\mathcal{A} = (Q_A,\ \Sigma,\ \chi,\ \delta_A,\ q_0,\ \perp,\ F)$. Let f be a symbol disjoint from Q_A. Let $Q = Q_A \cup \{f\}$ and

$$\delta = \{((q,\ \varepsilon,\ s),\ (f,\ \perp)) \mid q \in F,\ s \in \chi^*\} \cup \delta_A.$$

Suppose, in addition, that if $((q_1,\ w,\ s_1),\ (q_2,\ s_2)) \in \delta$, then $|s_2| = 1$. Let

$$\mathcal{B} = (Q,\ \Sigma,\ \chi,\ \delta,\ q_0,\ \perp,\ \{f\}).$$

If $w \in L$, then there is a path through $\mathcal{A}$, to a state in F, when reading w, so reading ε in addition, in B, takes us to f, so $w \in \mathscr{L}(\mathcal{B})$. If $w \in \mathscr{L}(\mathcal{B})$, then reading w can trace a path through b to f, which must go through a state in F, before reading the empty word. Hence $w \in L$. We can conclude that $\mathscr{L}(\mathcal{B}) = L$.

Let $V = Q \times \chi$ and

$$P = \{((q_2,\ s_2),\ (q_1,\ s_1)w) \mid ((q_1,\ w,\ s_1),\ (q_2,\ s_2)) \in \delta\} \cup \{((q_0,\ \perp),\ \varepsilon)\}.$$

Let $g = (V,\ \Sigma,\ P,\ (f,\ \perp))$. We have that g is a context free grammar. Let $w \in L$. Let $a_1a_2\cdots a_k = w$, where $k \in \mathbb{N}_0$ and $a_i \in \Sigma$ for all valid i. Then there is a sequence of transitions in δ, that are used when w is read to trace the path through $\mathcal{B}$. Let the sequence be

$$((q_0,\ a_1,\ s_0),\ (q_1,\ s_1)),\ ((q_1,\ a_2,\ s_1),\ (q_2,\ s_2)), \dots,\ ((q_{k-1}\ a_k,\ s_{k-1}),\ (q_k,\ s_k)).$$

We have that the stack starts off with just $\perp$, so $s_0 =\perp$. By construction of $\mathcal{B}$, we also have that $s_k =\perp$ and $q_k = f$. By construction of P, for each transition above, there exists a corresponding production. If we start at $(f,\ \perp)$, and use this sequence of productions in reverse, we have

$$\begin{aligned}(f,\ \perp) = (q_k,\ s_k) &\mapsto (q_{k-1},\ s_{k-1})a_k \mapsto (q_{k-2},\ s_{k-2})a_{k-1}a_k \\ &\mapsto \cdots \mapsto (q_0,\ s_0)a_1\cdots a_k = (q_0,\ \perp)a_1\cdots a_k \mapsto a_1\cdots a_k\end{aligned}$$

Hence $w \in \mathscr{L}(g)$.

Suppose now that $w \in \mathscr{L}(g)$. Let $a_1a_2\cdots a_k = w$, where $k \in \mathbb{N}_0$ and $a_i \in \Sigma$ for all valid i. We have that there is a sequence of productions in P that takes $(f,\ \perp)$ to w. This sequence must end with $((q_0,\ \perp),\ \varepsilon)$, otherwise w would contain non-terminals. In addition, the start symbol contains precisely one non-terminal, and every production in P, other than $((q_0,\ \perp),\ \varepsilon)$, preserves the number of non-terminals, so $((q_0,\ \perp),\ \varepsilon)$ is only used once. Therefore, there the sequence of productions, without the last production, corresponds to a sequence of transitions in δ. Let the reverse of this sequence be

$$((q_0,\ a_1,\ s_0),\ (q_1,\ s_1)),\ ((q_1,\ a_2,\ s_1),\ (q_2,\ s_2)), \dots,\ ((q_{k-1}\ a_k,\ s_{k-1}),\ (q_k,\ s_k)),$$

where $k \in \mathbb{N}_0$ and $(q_k,\ s_k) = (f,\ \perp)$. This sequence of transitions can be used when reading w, and traces a path through $\mathcal{B}$, from q_0 to q. Hence $w \in L$. We can conclude that $L = \mathscr{L}(g)$.

Theorem 4.4.8 *Let Σ be an alphabet and $L \subseteq \Sigma^*$. Then*

1. *If L is regular, then there exists $p \in \mathbb{N}_0$, such that for all $w \in L,\ |w| > p$, there exist words $r,\ s,\ t \in \Sigma^*$, such that*
$$w = rst, \quad |s| > 0, \quad rs^n \in L,$$
for all $n \in \mathbb{N}_0$,

2. *If L is context free, then there exists $p \in \mathbb{N}_0$, such that for all $w \in L,\ |w| > p$, there exist words $r,\ s,\ t,\ u,\ v \in \Sigma^*$, such that*
$$su > 0,\ |stu| \leq p + 1,\ rs^n tu^n v \in L,$$
for all $n \in \mathbb{N}_0$.

Definition 4.4.9 Let Σ be an alphabet and $w \in \Sigma^*$. A *contiguous substring* of w is a word $v \in \Sigma^*$, such that there exist words $x,\ y \in \Sigma^* \cup \{\varepsilon\}$, such that $w = xvy$.

Definition 4.4.10 Let $g = (V,\ \Sigma,\ P,\ S)$ be a context free grammar. Let $(z_i)_i \subseteq P$ be a finite chain of productions. Let i be a valid index and w be a contiguous substring of z_i. Let $j > i$ be a valid index. The *shadow* of w in z_j is the result of the string w, within z_j, after the sequence of productions have occurred.

The chain $(z_i)_i$ is called *efficient*, if whenever a non-terminal T appears in some word z_i for a valid index i, then T never appears in its own shadow.

Theorem 4.4.11 (Pumping Lemma for Context Free Languages) *Let L be a context free language over a finite alphabet Σ. Then there exists $p \in \mathbb{N}_0$, such that for all $z \in L$ such that $|z| \geq p$, there exist words $u,\ v,\ w,\ x,\ y \in \Sigma^*$, where*
$$z = uvwxy,\ |vx| > 0,\ |vwx| \leq p,$$
such that for all $n \in \mathbb{N}_0$,
$$uv^n wx^n y \in L.$$

Proof Let $g = (V,\ \Sigma,\ \pi,\ S)$ be a context free grammar for L. Let $X \subseteq L$ be the set of words in L, which can be produced using efficient chains of productions. Note that X is finite, since the set of non-terminals is finite, and a non-terminal can never appear in its own shadow.

Let r be the length of the longest word in X, and $p = r + 1$. If L has no words of length greater than or equal to p, then L is finite, and the theorem is true.

We will now consider when L is infinite. If $z \in L$ and $|z| \geq p$, so that $z \notin X$, then the chain of productions cannot be efficient. If we let $(x_n)_n$ be the shortest chain of productions producing z (from S), then being inefficient means that there are indices $i,\ j$, with $i < j$, and a non-terminal M, such that M is a contiguous subword of z_i and z_j, and M appears in its own shadow in z_j. We will call the shadow w_j, and break it down to write $v_j M x_j$, where at least one of v_j and x_j have non-trivial shadow in z. We will call these shadows v and x, and name the shadow of the M in z_j, in z as w. If they were trivial, then we could 'shorten' our chain.

Write $z_i = u_i M y_i$, and let u and y be the shadows of u_i and y_i in z, respectively. We therefore have that $z = uvwxy$. In addition, by replacing derivations of M with later derivations, we can conclude that, for any $n \in \mathbb{N}_0$,
$$uv^n wx^n y = z.$$

4.5 Context Free Languages and Groups

Definition 4.5.1 Let P be a property of groups. A group G is *virtually* P, if there is a finite index subgroup $H \leq G$, such that H has P.

We say G is *residually* P, if for all $g \in G \backslash \{1_G\}$, there is a group H_g and a homomorphism $\varphi_g : G \to H_g$, such that $\varphi_g(g) \neq 1_{H_g}$, and H_g has P.

Example 4.5.2 Every finite group is virtually trivial. A *virtually free group* is a group with a finite index free subgroup.

Theorem 4.5.3 *Free groups are residually finite.*

Example 4.5.4 Define $\mathcal{T}_2$ to be the infinite rooted binary tree. A subgroup $G \leq \mathrm{Aut}(\mathcal{T}_2) := H$ is residually finite.

Proof Let $\mathrm{Stab}_k(H)$ be the stabiliser of the $k$the row of H, where $k \in \mathbb{N}$. Note that $\mathrm{Stab}_k(H) \trianglelefteq H$, and

$$^{H}\!\diagup_{\mathrm{Stab}_k(H)},$$

is finite. Hence if $g \in H$ is non-trivial, with its first 'flip' on row k, then g has non-trivial image in

$$^{H}\!\diagup_{\mathrm{Stab}_k(H)}.$$

Definition 4.5.5 Let X and Y be metric spaces. A set function f from X to Y is called a *quasi-isometry*, if there exists $A \geq 1,\ B,\ C \geq 0$, such that for all $x_1,\ x_2 \in X$

$$\frac{1}{A} d_X(x_1,\ x_2) - B \leq d_Y(x_1 f,\ y_1 f) \leq A d_X(x_1,\ y_1) + B,$$

and for all $y \in Y$, there is an $x \in X$, such that

$$d_Y(y,\ xf) \leq C.$$

If such a function exists, then X and Y are called *quasi-isometric.*

Definition 4.5.6 Let G be a group, generated by a set X. Define a function

$$\begin{aligned} d : G \times G &\to [0, \infty) \\ (g,\ h) &\mapsto \min\{|w| \mid w \in W(X),\ gw = h\} \end{aligned}$$

Lemma 4.5.7 *The function defined in Definition 4.5.6, is a metric.*

Example 4.5.8 The groups F_a and $\langle b,\ c \mid [b,\ c] \rangle$ are not quasi-isometric.

Proof Let $G = \langle b,\ c \mid [b,\ c] \rangle$. Let d_1 be the induced metric on G, and d_2 be the induced metric on F_a.

Suppose they are quasi-isometric, and let $\phi : G \to F_a$ be the quasi-isometry, with constants $A,\ B,\ C$, defined as in the definition. Let $l \in \mathbb{Z}$ such that $a^l = \varepsilon\phi$. Redefine ϕ, and $A,\ B,\ C$, by composing ϕ with the isometry of F_a: $a^k \mapsto a^{k-l}$, to assume $\varepsilon\phi = \varepsilon$.

Claim: If $g,\ h \in G$ such that $A^2 d_1(g,\ \varepsilon) + 2AB \leq d_1(h,\ \varepsilon)$, then $d_2(g\phi,\ \varepsilon) \leq d_2(h\phi,\ \varepsilon)$.

Note
$$A^2 d_1(g,\ \varepsilon) + 2AB \leq d_1(h,\ \varepsilon) \implies d_1(g,\ \varepsilon) \leq \frac{d_1(h,\ \varepsilon)}{A^2} - \frac{2B}{A}. \tag{4.2}$$
We have
$$\begin{aligned} d_2(g\phi,\ \varepsilon) &\leq A d_1(g,\ \varepsilon) + B \\ &\leq \frac{d_1(h,\ \varepsilon)}{A} - B \\ &\leq \frac{A d_2(h\phi,\ \varepsilon) + B}{A} - B \\ &\leq \frac{A d_2(h\phi,\ \varepsilon) + AB}{A} - B \\ &= d_2(h\phi,\ \varepsilon), \end{aligned}$$
and the claim is true.

Let $n \in \mathbb{N}_0$. Let $k_n = n(A^2 + 2AB)$. We have
$$d_1(b^{nk_n},\ \varepsilon) = nk_n.$$
Therefore, if $i,\ j \in \mathbb{Z}$ such that $|i| + |j| \leq n$, then
$$A^2 d_1(b^i c^j,\ \varepsilon) + 2AB \leq nA^2 + 2AB = d_1(b^{nk_n},\ \varepsilon).$$
We have $2N + 1$ choices for i. Given i, there are $2(n - |i|) + 1$ choices for j. Let K be the number of elements of G that are of the form $b^i c^j$, where $i,\ j \in \mathbb{Z}$, with $|i| + |j| \leq n$. Then
$$\begin{aligned} K &= \sum_{i=-n}^{n} (2(n - |i|) + 1) \\ &= 2n + 1 + 2 \sum_{i=-n}^{n} (n - i) \\ &= 2n + 1 + 2(2n+1)n - 2 \sum_{i=-n}^{n} |i| \\ &= 4n^2 + 4n + 1 - 4 \sum_{i=1}^{n} i + |0| \\ &= 4n^2 + 4n + 1 - 2n(n+1) \\ &= 2n^2 + 2n + 1 \end{aligned}$$
Hence, using claim, there are $2n^2 + 2n + 1$ elements g of G such that
$$d_2(g\phi,\ \varepsilon) \leq d_2(b^{k_n}\phi,\ \varepsilon).$$
Let $l_n \in \mathbb{Z}$, such that $a^{l_n} = (b^{k_n})\phi$. We have that there are at least $2n^2 + 2n + 1$ elements in $B_2(\varepsilon,\ |l_n|)$. We subscript B by 2, to denote we are using d_2. There are $2|l_n| + 1$ elements in $B_2(\varepsilon,\ |l_n|)$, which are
$$\{a^m \mid m \in \mathbb{Z},\ |m| \leq |l_n|\}.$$

Let $g,\ h \in G$ such that $g\phi = h\phi$. Then

$$\frac{d_1(g,\ h)}{A} - B \leq 0 \implies d_1(g,\ h) \leq AB.$$

We can conclude that if $g,\ h \in G$ and $d_1(g,\ h) > AB$, then $g\phi \neq h\phi$. We will use this to find a lower bound for the number of distinct elements of $B_2(\varepsilon,\ |l_n|)$. Let $K = \lceil AB \rceil$. Then $b^{nK},\ c^{nK},\ \varepsilon$ have distinct images from each other, for $n \in \mathbb{Z}\backslash\{0\}$. Hence $|l_n| \geq 2\left\lfloor \frac{n^2+n}{K} \right\rfloor$. We have that

$$\frac{2(n^2+n)}{K} - 1 \leq |l_n| = d_2(a^{l_n},\ \varepsilon) \leq Ad_1(b^{k_n},\ \varepsilon) + B = Ak_n + B = n(A^3 + 2A^2B) + B.$$

If $n \geq K(A^3 + 2A^2B + B + 1)$, then

$$K(A^3 + 2A^2B + B + 1)^2 + A^3 + 2A^2B + B + 1 \leq (A^3 + 2A^2B + B)^2 + B,$$

a contradiction. Hence ϕ does not exist, and the groups are not quasi-isometric.

Proof ($\Rightarrow$): Suppose G is finitely generated. Let X'_G be a finite generating set for G. Let $X_G = \{g \in G \mid \{g,\ g^{-1}\} \cap X'_G \neq \emptyset\}$, ie the X'_G union its inverses. Let $n = |X_G|$, and name the elements of X_G by

$$X_G = \{g_1,\ \ldots, g_n\}.$$

Let $T = \{t_1,\ t_2,\ \ldots,\ t_s\}$, where $s = [H : G] < \infty$, by a traversal of H by G

Let $h \in H$. We have that $h \in Gt_i$, for some valid index i, and hence

$$h = g_1 g_2 \cdots g_n t_i,$$

Since h was arbitrary, we have that $H = \langle T \cup X_G \rangle$.

($\Leftarrow$): Suppose H is finitely generated. Let $X_H = \{h_1,\ h_2,\ \ldots,\ h_n\}$ be a finite generating set for H, closed under inverses. Let $T = \{t_1,\ t_2,\ \ldots, t_s\}$, where $s = [H : G]$, be a traversal for G in H. For each valid index i, define $i\theta \in \mathbb{N}$ and $g_i \in G$ by $h_i = g_i t_{i\theta}$. Set $g_{i,\ j} \in G,\ t_{i,j} \in T$, such that

$$\begin{aligned} t_i g_i &= g_{i,j} t_{i,j} \\ t_i t_j &= \tilde{g}_{i,j} \tilde{t}_{i,j} \end{aligned}$$

Let $h \in H$. Then, there exists $k \in \mathbb{N}$, and a function $\psi : \mathbb{N} \to \mathbb{N}$, such that

$$\begin{aligned} h &= h_{1\psi} h_{2\psi} \cdots h_{k\psi} \\ &= g_{1\psi} t_{1\psi\theta} g_{2\psi} t_{2\psi\theta} \cdots g_{k\psi} t_{k\psi\theta} \\ &= g_{1\psi} g_{1\psi\theta,2\psi} t_{1\psi\theta,2\psi} \cdots g_{k\psi} t_{k\psi\theta} \\ &= \cdots \\ &= \hat{g}_1 \hat{g}_2 \cdots \hat{g}_k \hat{t}, \end{aligned}$$

and if $h \in G$, then $\hat{t} = 1_H$. Therefore G is finitely generated by $\{\hat{g}_1 \cdots \hat{g}_k\}$.

Theorem 4.5.9 (Muller-Schupp (half)) *Let H be a virtually free group, generated by a finite set X. Then* $\mathrm{WP}(H,\ X)$ *is a context free language.*

Proof (Outline) There is a subgroup $\tilde{N} \trianglelefteq H$, which is normal (Poincaré's Lemma) and free (subgroup of a free group), such that $[H : N] < \infty$. Let N be a maximal such subgroup. There are maps

$$N \rightarrowtail H \twoheadrightarrow Q := {}^{H}\!/\!_{N}.$$

By Schreier's Lemma, N is finitely generated, and hence $N = F_{x_1,\ \ldots,\ x_k}$. Let Y be the inverse closure of $\{x_1,\ \ldots,\ x_k\}$. We will build a pushdown automaton with alphabet Y and states Q. The accept and start state will be 1_Q. The traversal for N in H will define the transition relation.

Definition 4.5.10 A group G is *context free* if $\mathrm{WP}(G,\ X)$ is a context free language, for any generating set X for G.

Lemma 4.5.11 *Suppose G is a finitely generated group and $H \leq G$, with $[G : H] < \infty$. If H is context free, then G is context free.*

Proof (Sketch) Let X be a finite generating set for H such that $\mathrm{WP}(H,\ X)$ is a context free language. Then there is an automaton $\mathcal{A}$, such that $\mathcal{A}$ accepts $\mathrm{WP}(H,\ X)$. We also have that there is a transversal$T = \{1_G = t_1,\ t_2,\ \ldots, t_n\}$, for H in G. In addition, there is a finite generating set $X \cup \tilde{X} \cup T$ for G, where $\tilde{X} \subseteq H$ is defined in the proof of Schreier's Lemma. Note $X \cup \tilde{X}$ is a finite generating set for H. Build a new automaton $\tilde{\mathcal{A}}$ from $\mathcal{A}$, to accept $\mathrm{WP}(H,\ X \cup \tilde{X})$. To do this read letters in X as in $\tilde{A}$, but instead of reading letters in $\tilde{X}$, read the correct word from X in $\mathcal{A}$. Build a new automaton

$$B = (Q,\ Y,\ \chi_{\tilde{A}}, \tilde{\delta},\ q_0,\ \perp,\ F),$$

where

$$Q = Q_{\tilde{\mathcal{A}}} \times T, \quad q_0 = (\mathrm{start}_{\tilde{\mathcal{A}}},\ 1_H), \quad F = \{(\mathrm{accept}_{\tilde{\mathcal{A}}},\ 1_H)\}.$$

Define $\tilde{\delta}$, so that movement occurs in cosets space (2nd coordinate), and in $\tilde{\mathcal{A}}$ simultaneously.

Lemma 4.5.12 *Let G be a context free group, generated by a finite set X, such that* $\mathrm{WP}(G,\ X)$ *is context free. Then if Y is a finite generating set for G,* $\mathrm{WP}(G,\ Y)$ *is context free.*

Proof We have already shown that if $\mathrm{WP}(G,\ A)$ is context free, then $\mathrm{WP}(G,\ A \cup B)$ is, for any finite $B \subseteq G$. Let $\mathcal{A}$ be a pushdown automaton accepting $\mathrm{WP}(G,\ X \cup Y)$, built in the proof of the previous Lemma. Remove all transitions for reading letters from $X \backslash Y$, and the new automaton accepts $\mathrm{WP}(G,\ Y)$.

Lemma 4.5.13 *Let G be a context free group, generated by a finite set X. Let $Y \subseteq G$ be finite. Then $\langle Y \rangle$ is a context free group.*

Theorem 4.5.14 (Motz Isomorphism) *Let $g = (V,\ \Sigma,\ P, \S)$ be a context free grammar. Let $L = \mathscr{L}(g)$, with $\varepsilon \in L$. Then the inclusion of Σ^* into $F_{V \cup \Sigma}$ induces a canonical isomorphism*

$$\phi : {}^{F_\Sigma}\!/\!_{\langle\langle L \rangle\rangle} \to {}^{F_{V\cup\Sigma}}\!/\!_{\langle\langle P \rangle\rangle}.$$

Corollary 4.5.15 *Context free groups are finitely presented.*

Chapter 5

Bass Serre Theory

5.1 Free Products

Definition 5.1.1 Let A, B and C be (formally disjoint) groups such that there exist monomorphisms $\psi_A : C \to A$ and $\psi_B : C \to B$. Let X_A and X_B be generating sets for A and B, respectively. Define the *free product with amalgamation* of A and B by C, denoted $A *_C B$, by

$$A *_C B = \langle X_A \cup X_B \cup X_C \mid R_A \cup R_B \cup \{g^{-1}(g)\psi_A \mid g \in C\backslash\{1_C\}\} \cup \{g^{-1}(g)\psi_B \mid g \in C\backslash\{1_C\}\}\rangle.$$

Note that this is not always unique (given the notation), since the monomorphisms may be non-unique.

Let I be an index set, and $G_i = \langle X_i,\ R_i\rangle$ be groups, for all $i \in I$. Then the *free product* of the G_is is defined as

$$\mathop{*}_{i\in I} G_i = \left\langle \bigcup_{i\in I} X_i \;\middle|\; \bigcup_{i\in I} R_i \right\rangle.$$

Example 5.1.2 Consider

$$\begin{aligned} D_8 &= \langle \sigma,\ \tau \mid \sigma^4,\ \tau^2,\ (\sigma\tau)^2\rangle, \\ D_6 &= \langle \rho,\ \mu \mid \rho^3,\ \mu^2,\ (\rho\mu)^2\rangle, \\ C &= \langle c \mid c^2\rangle. \end{aligned}$$

Note

$$\begin{aligned} \psi_{D_8} : C &\to D_8 \\ c &\mapsto \tau \\ \psi_{D_6} : C &\to D_6 \\ c &\mapsto \mu, \end{aligned}$$

extend to homomorphisms, using Von Dyck's Theorem. Then

$$\begin{aligned} D_8 *_C D_6 &= \langle \sigma,\ \tau,\ \rho,\ \mu,\ c \mid \sigma^4,\ \tau^2,\ (\sigma\tau)^2,\ \rho^3,\ \mu^2,\ (\rho\mu)^3,\ c^{-1}\tau,\ c^{-1}\mu\rangle \\ &\mapsto_{T_4} \langle \sigma,\ \tau,\ \rho,\ \mu \mid \sigma^4,\ \tau^2,\ (\sigma\tau)^2,\ \rho^3,\ \mu^2,\ (\rho\mu)^3,\ \mu\tau,\ \mu\mu\rangle \\ &\mapsto_{T_2} \langle \sigma,\ \tau,\ \rho,\ \mu \mid \sigma^4,\ \tau^2,\ (\sigma\tau)^2,\ \rho^3,\ \mu^2,\ (\rho\mu)^3,\ \mu\tau\rangle \end{aligned}$$

Theorem 5.1.3 *Let G_i be groups with normal forms, for all $i \in I$, where I is an index set. Consider an element of $H = *_{i \in I} G_i$ of the form*

$$g = g_1 g_2 \cdots g_k,$$

for some $k \in \mathbb{N}$. Consider, for all $i \in I$, the following statements.

1. *There is an index α_i, such that $g_i \in G_{\alpha_i}$,*
2. *$g_i \neq 1_{\alpha_i}$,*
3. *g_i is in the normal form of G_{α_i},*
4. *$\alpha_i \neq \alpha_{i+1}$.*

If 1, 2 and 4 are satisfied, then g is non-trivial. If, in addition, 3 is satisfied, then this is a normal form for non-trivial elements of H.

5.2 HNN Extensions

Definition 5.2.1 Let $A = \langle X_A | R_A \rangle$, where X_A is a set, and $R_A \subseteq W(X_A)$. Let $H,\ K \leq A$, such that there is an isomorphism $\psi : H \to K$. Let X_H be a generating set for H. Let t be a symbol not in $W(X)$. The *HNN extension* of A with respect to ψ, denoted $A*_\psi$, is defined by

$$A*_\psi = \langle X_A \cup \{t\} \mid R_A \cup \{t^{-1}ht(h\psi)^{-1} \mid h \in X_H\} \rangle.$$

Lemma 5.2.2 (Britton's Lemma) *Let A be a group, and $H,\ K \leq A$, such that there is an isomorphism $\psi : H \to K$. Let $G = A*_\psi$. Let $w \in G$ be of the form*

$$w = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} \cdots t^{\varepsilon_n} g_n,$$

where $n \in \mathbb{N}_0,\ g_i \in G,\ \varepsilon_j \in \{-1,\ 1\}$, for valid indices i and j. If $w =_G 1_G$, then precisely one of the following holds:

1. *$n = 0$ and $g_0 = 1_G$,*
2. *$n > 0$, and for some $i \in \{1,\ \ldots,\ n-1\}$, one of the following holds:*
   (a) *$\varepsilon_i = -1,\ \varepsilon_{i+1} = 1,\ g_i \in H$,*
   (b) *$\varepsilon_i = 1,\ \varepsilon_{i+1} = -1,\ g_i \in K$.*

Remark 5.2.3 Britton's Lemma gives a pseudo-normal form.

Example 5.2.4 Let $G = \langle a,\ b \mid a^2,\ b^3,\ (ab)^2 \rangle \cong S_3$. A normal form for G is

$$\{\varepsilon,\ a,\ b,\ ab,\ b^2,\ ab^2\},$$

under the rewrite rules

$$a^{-1} \mapsto a,\ b^{-1} \mapsto b^2,\ b^3 \mapsto \varepsilon,\ a^2 \mapsto \varepsilon,\ ba \mapsto ab^2.$$

We have $|a| = 2 = |ab^2|$. Note $a \neq ab^2$. So we have two different subgroups of G:

$$\langle a \rangle, \quad \langle ab^2 \rangle,$$

both isomorphic to C_2. Note that

$$\begin{aligned} \psi : \langle a \rangle &\to \langle ab^2 \rangle \\ a &\mapsto ab^2 \\ \varepsilon &\mapsto \varepsilon, \end{aligned}$$

is an isomorphism. Then

$$\begin{aligned} G*_\psi &= \langle a,\ b,\ t \mid a^2,\ b^3,\ (ab)^2,\ t^{-1}atb^{-2}a^{-1} \rangle \\ &\cong \langle a,\ b,\ t \mid a^2,\ b^3,\ (ab)^2,\ t^{-1}atab^2 \rangle \end{aligned}$$

Note that t has infinite order, so $|G *_\psi|$ is infinite. Consider

$$\begin{aligned} w &= abtb^{-1}a^{-1}taat^{-1}bt^{-1}a^{-1}tt \\ &=_G abtb^{-1}a^{-1}tt^{-1}bt^{-1}a^{-1}tt \\ &=_G abtb^{-1}a^{-1}bt^{-1}a^{-1}tt \\ &=_G abtab^2t^{-1}att \end{aligned}$$

Note $tab^2t^{-1} =_G tt^{-1}att^{-1} =_G a$, so

$$\begin{aligned} w &=_G abaatt \\ &=_G abtt \neq 1_G, \end{aligned}$$

by Britton's Lemma.

5.3 Graphs of Groups

Definition 5.3.1 A *graph of groups* is a pair $\mathscr{G} = (\mathbb{G},\ \Gamma)$, where $\Gamma = (V,\ E,\ s,\ t)$ is a digraph with an involution function$^-$: $E \to E$, such that $\bar{e}$ is defined to be an edge $f \in E$, such that $et = fs$ and $ft = es$, and where $\mathbb{G} = (\{G_x \mid x \in V \cup E\},\ \{\alpha_e : G_e \to G_{es} \mid e \in E\})$. Here, all elements of the first set of $\mathbb{G}$ must be groups, and this set must be associated bijectively with $V \cup E$. The second set contains injective group homomorphisms from each edge group into the vertex group at the start of the edge. Finally, there is the condition that $G_e = G_{\bar{e}}$, for any edge e.

Definition 5.3.2 Let $\mathscr{G} = (\mathbb{G},\ \Gamma)$ be a graph of groups, where $\Gamma = (V,\ E,\ s,\ t)$. Let T be a spanning tree for Γ. Let the groups G_x in the set of $\mathbb{G}$, have presentations $\langle X_x | R_x \rangle$. Define

$$\pi_1(\mathscr{G}) = \left\langle \bigcup_{v \in V} X_v \cup E \mid \{e\bar{e},\ \bar{e}e \mid e \in E\} \cup \bigcup_{v \in V} R_v \cup \{\bar{e}(x\alpha_e)e(x\alpha_{\bar{e}})^{-1} \mid x \in X_{es}\} \cup \{e \mid e \in T\} \right\rangle.$$

Chapter 6

Linear Groups and the Ping-Pong Lemma

6.1 The Modular Group

Definition 6.1.1 Let $n \in \mathbb{N}$. Consider the general liner group $\mathrm{GL}_n(\mathbb{Z})$, and the special linear group $\mathrm{SL}_n(\mathbb{Z})$, over $\mathbb{Z}$. Note that elements of $\mathrm{GL}_n(\mathbb{Z})$ have determinant ± 1. Let $\mathscr{D}$ denote the subgroup of $\mathrm{GL}_n(\mathbb{Z})$, generated by the diagonal matrices. We have that

$$\mathscr{D} = Z(G).$$

In addition, we have that $\mathscr{D} \cap \mathrm{SL}_n(\mathbb{Z}) \trianglelefteq \mathrm{SL}_n(\mathbb{Z})$. Define

$$\mathrm{PSL}_n(\mathbb{Z} = {}^{SL_n(\mathbb{Z})}\!\big/_{\mathscr{D} \cap \mathrm{SL}_n(\mathbb{Z})}.$$

We will call $\mathrm{PSL}_2(\mathbb{Z})$ the *modular group.*

Theorem 6.1.2 *Let*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then

$$\mathrm{PSL}_2(\mathbb{Z}) = \langle s,\ t \rangle.$$

Proof (sketch) Note that $\mathrm{PSL}_2(\mathbb{Z})$ can be viewed as $\mathrm{SL}_2(\mathbb{Z})$, under the equivalence relation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \sim \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}.$$

The proof requires applying 'the Euclidean algorithm'

Lemma 6.1.3 *The group* $\mathrm{GL}_n(\mathbb{Z})$ *is residually finite, for any* $n \in \mathbb{N}$.

Proof Let $n \in \mathbb{N}$. Define, for any prime p,

$$\varphi_p : \mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{F}_p)$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \mapsto \begin{pmatrix} a_{11} \mod p & a_{12} \mod p & \cdots & a_{1n} \mod p \\ a_{21} \mod p & a_{22} \mod p & \cdots & a_{2n} \mod p \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} \mod p & a_{n2} \mod p & \cdots & a_{nn} \mod p \end{pmatrix}$$

Let $A,\ B \in \mathrm{GL}_n(\mathbb{Z})$. For any valid i and j and any prime p, let the ijth entries of $A,\ B,\ AB,\ A\varphi_p,\ B\varphi_p$ and $(A\varphi_p)(B\varphi_p)$, be $a_{ij},\ b_{ij},\ c_{ij},\ \alpha_{ij},\ \beta_{ij}$ and γ_{ij}, respectively. We have, for any valid i and j,

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Let p be prime. Given valid i and j, we also have

$$\gamma_{ij} = \sum_{k=1}^{n} \alpha_{ik} \beta_{kj}.$$

Noting that applying $\mod$ respects addition and multiplication, it follows that

$$\begin{aligned}
\gamma_{ij} &= \sum_{k=1}^{n} \alpha_{ik} \beta_{kj} \\
&= \sum_{k=1}^{n} (a_{ik} \mod p)(b_{kj} \mod p) \\
&= \sum_{k=1}^{n} a_{ik} b_{kj} \mod p \\
&= \left(\sum_{k=1}^{n} a_{ik} b_{kj} \right) \mod p \\
&= c_{ij} \mod p,
\end{aligned}$$

which is the ijth entry of $(AB)\varphi_p$. It follows that every entry of $(AB)\varphi_p$ and $(A\varphi_p)(B\varphi_p)$ are the same, and hence φ_p is a homomorphism.

Let $A \in \mathrm{GL}_n(\mathbb{Z})$ have ijth entry a_{ij}, for any valid i and j. If $A \neq I_n$, then there exists $i,\ j \in \mathbb{N},\ i,\ j \leq n$, such that $a_{ij} \neq 1$, if $i = j$, and $a_{ij} \neq 0$, if $i \neq j$. Let p be a prime number strictly greater than a_{ij}. Then the ijth entry of $A\varphi_p$, has the same name as a_{ij}, which is not that of 1 if $i = j$ and 0, if $i \neq j$. We can conclude that $A\varphi_p \neq I_n$, as they differ in the ijth entry. Note also that $\mathrm{GL}_n(\mathbb{F}_p)$ is finite for any prime p. We can conclude that $\mathrm{GL}_n(\mathbb{Z})$ is residually finite.

6.2 The Ping-Pong Lemma

Theorem 6.2.1 (Ping-Pong Lemma) *Let G be a group, acting on a set X. Let $G_1,\ G_2 \leq G$, such that $|G_1| > 1$ and $|G_2| > 2$. Let $X_1,\ X_2 \subseteq X$, such that $X_1 \not\subseteq X_2$. Define $H = \langle G_1,\ G_2 \rangle$. Suppose that*

1. *For all $x_1 \in X_1,\ g_2 \in G_2 \backslash \{1_G\}$, we have $x_1 g_2 \in X_2$,*
2. *For all $x_2 \in X_2,\ g_1 \in G_1 \backslash \{1_G\}$, we have $x_2 g_1 \in X_1$.*

Then $H \cong G_1 * G_2$, and that exists an isomomorphism that maps an alternating product

$$g_{11} g_{21} g_{12} g_{22} \cdots g_{1n} g_{2n},$$

to the same named product in $G_1 * G_2$. Here, $g_{1i} \in G_j,\ g_{2i} \in G_{(j \mod 2)+1}$ for all valid i, and some $j \in \{1,\ 2\}$.

Proof Let

$$g = g_1 g_2 \cdots g_n \in H,$$

for some $n \in \mathbb{N}$, and such that for any valid i, we have $g_i \in G_j$ and $G_{i+1} \notin G_j$, for some $j \in \{1,\ 2\}$. That is, this is an alternating product. We now need to show that if g_i is non-trivial for all valid i, then g is non-trivial. Suppose g_i is non-trivial for all valid i. Recall that conjugation by any element does not change whether or not an element is trivial. We will conjugate g, in order to assume $g_1,\ g_n \in G_2$.

If $g_1,\ g_n \in G_2$, then we do not need to conjugate. If $g_1,\ g_n \in G_1$, then conjugating by a non-trivial element $h \in G_2$ will yield an alternating product of length $n+2$, whose first and last elements are non-trivial and in G_2. If precisely one of g_1 and g_2 is in G_2, then we can conjugate by a non-trivial element $h \in G_2$, that is not the inverse of whichever of $g_1,\ g_2$ is in G_2. We will end up with an alternating product of length $n+1$, with non-trivial elements of G_2 at each end.

We can now assume $g_1,\ g_n \in G_2$. Let $x \in X_1 \backslash X_2$, which exists by the assumptions in the theorem. Since the alternating product starts and ends with elements of G_2, we must have that n is odd. We also have that for each odd i, $g_i \in G_2$ and for even, $g_i \in G_1$. Hence applying $g_1 g_2 \cdots g_n$, will move x to X_2, and back to X_1 n times, which will result in $xg \in X_2$, since n is odd. Since $x \notin X_2$, we have that $xg \neq x$, and hence g is non-trivial.

We now have that every non-trivial element of H can be written in the normal form for $G_1 * G_2$, as in Theorem 5.1.3. Let $\phi : G_1 * G_2 \to H$ map alternating products in $G_1 * G_2$ to products of the same name in H, and send the identity to the identity. This is a bijection, since the normal form covers all elements of H, and the kernel is the identity. In addition, for any $h_1,\ h_2 \in G_1 * G$, then $h_1 h_2$ will already be in the normal form, subject to some cancellations at the end, which can be added back in, in H. It is therefore a homomorphism.