# Geometric Group Theory

Notes by Zach Schutzman

University of Pennsylvania, Fall 2017

# Introduction

Taking notes and working through proofs is the best way for me to teach myself advanced mathematics. Typing (and thoroughly backing up) notes is the best way to make sure they are preserved and readable well into the future. As such, these notes are from my process of working through *Topics in Geometric Group Theory* by Pierre de la Harpe.

These notes are being written intermittently, as learning Geometric Group Theory is something that must come after my required coursework, research, and teaching. I am using the editor TeXstudio. The template for these notes was created by Zev Chonoles and is made available (and being used here) under a Creative Commons License.

I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to Professor de la Harpe and those mathematicians he references.

Please email any corrections or suggestions to ianzach+notes@seas.upenn.edu.

# Chapter 1

## The Gauss Circle Problem

Suppose we have a circle of radius $\sqrt{t}$ in $\mathbb{Z}^2$ centered at the origin. How many lattice points are contained in the circle. That is, we are interested in

$$R(t) = \#\{(a,b) \in \mathbb{Z}^2 | (a^2 + b^2) \leq t\}$$

Right away, we can see things like $R(0) = 1$, as this 'circle' contains only the origin. We also have $R(1) = 5$, as this circle contains the origin and the four points $(1,0), (0,1), (-1,0), (0,-1)$. We'd like to understand $R(t)$ as $t$ grows large.

The book also tells us that:

$$\begin{aligned} R(10) &= 37 & \qquad R(1000) &= 3149 \\ r(100) &= 317 & \qquad R(10000) &= 31417 \end{aligned}$$

A pretty obvious pattern emerges here: we can see that $R(10^k) \approx \pi \cdot 10^k$, furthermore, $R(t) \approx \pi t$.

**Theorem.** *(Gauss)*

*Asymptotically,* $R(t) - \pi t = O(\sqrt{t})$.

*Proof.* Throughout, assume that $t \geq 0$. To each point $(a,b) \in \mathbb{Z}^2$, we associate the axis-aligned unit square which has $(a,b)$ as its 'southwest' corner. If $a^2 + b^2 \leq t$, then expanding the radius slightly to $\sqrt{t} + \sqrt{2}$ ensures the entire square associated with $(a,b)$ sits inside of the circle. This may add more points to the circle, as $R(t) \leq R(t+k)$ for $k \geq 0$ by construction. Thus we have

$$R(t) \leq \pi(\sqrt{t} + \sqrt{2})$$

The right-hand side of this inequality is the area of the expanded circle which contains all of the squares associated with points in our original circle of radius $\sqrt{t}$, so it must at least contain all of the southwest corners of those squares, and therefore at least all of the points in the original circle.

Conversely, if the square associated to $(a,b)$ touches the circle of radius $\sqrt{t} - \sqrt{2}$, then it must be the case that $a^2 + b^2 \leq t$. We can see this by thinking about a square which touches the smaller circle, but whose point $(a,b)$ is not contained in that circle. How far away can $(a,b)$ be from the smaller circle? The answer is $\sqrt{2}$, as in the worst case, the square sits in the lower-left quadrant and its northeast corner barely touches the circle. Expanding the circle's radius by $\sqrt{2}$ puts the southwest corner inside the circle. By the same argument as before, we have that

$$R(t) \geq \pi(\sqrt{t} - \sqrt{2})^2$$

Now we have two inequalities which look kind of symmetric, expanding the binomials and rearranging gives us

$$|R(t) - \pi t| \leq 2\pi(1 + \sqrt{2t})$$

This quantity on the right is asymptotically in $O(\sqrt{t})$, and we are done.

□

See the text for some references to improved bounds and generalizations of this problem.

## Pólya's Recurrence Theorem

**Definition.** A **simple random walk** is one in which the steps are all of length one and they are chosen independently from a fixed distribution.

**Definition.** A **symmetric** simple random walk is one in which the probability of taking some step $\alpha$ is equal to the probability of taking the inverse step $\alpha^{-1}$.

**Definition.** A walk is called **recurrent** if with probability 1 it visits the starting point infinitely often.

Let's think about the symmetric random walk on the integers $\mathbb{Z}$ where we start at the origin 0 and at each step we more left $(-1)$ with probability .5 and right $(+1)$ with probability .5. A natural question to ask is whether this walk is recurrent. Note that for random walks on structures that look like $\mathbb{Z}^k$ we'll always assume that we start at the origin unless otherwise specified.

**Claim.** The simple symmetric random walk on $\mathbb{Z}$ is recurrent.

*Proof.* We proceed combinatorially. The number of total walks of length $2n$ is $2^{2n}$. We can see this by thinking of a walk as a binary string, using 0 for a move left and 1 for a move right. There are $2^k$ such strings of length $k$. Next, we can see that the number of walks of length $2n$ which end at the origin are $\binom{2n}{n}$, as such a walk consists of exactly $n$ steps left and $n$ steps right, which we can specify by identifying at which times we moved left.

Let $u_{2n}$ be the probability that a walk of length $2n$ chosen uniformly at random ends at the origin. Thus

$$u_{2n} = \frac{1}{2^{2n}}\binom{2n}{n} = \frac{1}{2^{2n}}\frac{(2n)!}{n! \cdot n!}$$

Observe that walks of odd length never end at the origin, so $u_k$ for odd $k$ is zero.

Stirling's approximation[1] tells us that $m! \approx m^m e^{-m}\sqrt{2\pi m}$, and plugging this into the above probability $u_{2n}$ gives us

$$u_{2n} \approx \frac{1}{2^{2n}}\frac{(2n)^{2n}e^{-2n}\sqrt{2\pi 2n}}{n^{2n}e^{-2n}2\pi n} = \frac{1}{\sqrt{\pi n}}$$

Now, for a walk to be recurrent, we want to examine the sum over all walk lengths of the probability of that walk ending at the origin.

Since $\sum_{n=1}^{\infty} \frac{1}{\sqrt{n}} = \infty$, we have that

$$\sum_{k=1}^{\infty} u_k = \sum_{n=1}^{\infty} u_{2n} = \sum_{n=1}^{\infty} \frac{1}{\sqrt{\pi n}} = \frac{1}{\sqrt{\pi}}\sum_{n=1}^{\infty}\frac{1}{\sqrt{n}} = \infty$$

So the simple symmetric random walk on $\mathbb{Z}$ revisits the origin infinitely often with probability 1.

□

[1] In Stirling's approximation, $\approx$ means that the ratio of the quantities on the left-hand and right-hand side approaches 1 as we take a limit as $m$ goes to infinity.

**Claim.** Let $\{a_n\}_{n\in\mathbb{N}}$ be a sequence of numbers such that $0 \leq a_i \leq 1$ for all $i \in \mathbb{N}$. The infinite product $\prod_{n=1}^{\infty}(1-a_n)$ converges to a real number (between zero and one) if and only if the infinite sum $\sum_{n=1}^{\infty}$ converges.

*Proof.* Take the logarithm of the infinite product to turn it into the sum

$$\log\left(\prod_{n=1}^{\infty}(1-a_n)\right) = \sum_{n=1}^{\infty}\log\left(1-a_n\right)$$

which converges if and only if the original product does. We have from calculus that

$$\lim_{x\to 0}\frac{\log(1-x)}{x} = -1$$

so assuming that the sequence $\{a_n\}_{n\in\mathbb{N}}$ goes to zero as $n$ grows (which is a bare-minimum requirement for convergence of the series), we have that

$$\lim_{n\to\infty}\frac{\log(1-a_n)}{a_n} = -1$$

And by a comparison test, this series converges exactly when $\sum_{n=1}^{\infty}$ does. □

This tells us that a random walk is recurrent if and only if the probability of never revisiting the origin is zero (we'll plug in $u_k$ for $a_n$ and check if the product diverges to zero.)

What about walks on $\mathbb{Z}^2$? Now we'll consider the symmetric simple random walk where we move up, down, left, or right by one unit with equal probability at each time step. Is this walk recurrent?

The number of paths of length $2^{2n}$ is now $4^{2n}$, and for a walk to revisit the origin, we must have $k$ steps each north and south and $n-k$ steps each east and west. The number of these is described by the multinomial coefficient

$$\binom{2n}{k,k,n-k,n-k} =$$

$$= \binom{2n}{k}\binom{2n-k}{k}\binom{2n-2k}{n-k}$$

$$= \frac{(2n)!\cdot(2n-k)!\cdot(2n-2k)!}{(2n-k)!\cdot k!\cdot(2n-2k)!\cdot k!\cdot(n-k)!\cdot(n-k)!}$$

$$= \frac{(2n)!}{k!\cdot k!\cdot(n-k)!\cdot(n-k)!}$$

Then, the probability $u_{2n}$ of being at the origin after $2n$ steps is

$$u_{2n} = \frac{1}{4^{2n}} \sum_{k=0}^{n} \frac{(2n)!}{k! \cdot k! \cdot (n-k)! \cdot (n-k)!} = \frac{1}{4^{2n}} \frac{(2n)!}{n! \cdot n!} \sum_{k=1}^{n} \binom{n}{k} \binom{n}{n-k}$$

From the combinatorics, we have the identity $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}$. We can think of the first quantity as counting the number of binary strings of length $2n$ with exactly $n$ zeros and the second as all of the ways to form a pair of binary strings of length $n$, the first with $k$ zeros and the second with $n-k$ zeros, for a total of $n$ zeros across the two strings. From here, the bijection is easy to see.

So we have

$$u_{2n} = \frac{1}{4^{2n}} \frac{(2n)!}{n! \cdot n!} \binom{2n}{n}$$

and by Stirling's approximation, we have

$$u_{2n} \approx \frac{1}{\pi n} \; and \; \sum_{n=1}^{\infty} u_{2n} = \infty$$

so such walks on $\mathbb{Z}^2$ are recurrent.

Naturally, we now want to ask the same question about $\mathbb{Z}^3$. It turns out, such walks are transient.

**Definition.** A walk is called **transient** if it is not recurrent.

Skipping the redundant work, on $\mathbb{Z}^3$, we have

$$u_{2n} = \frac{1}{6^{2n}} \sum_{\substack{j,k \geq 0 \\ j+k \leq n}} \frac{(2n)!}{j! \cdot j! \cdot k! \cdot k! \cdot (n-j-k)! \cdot (n-j-k)!}$$

$$= \frac{1}{2^{2n}} \binom{2n}{n} \sum_{\substack{j,k \geq 0 \\ j+k \leq n}} \left( \frac{1}{3^n} \frac{n!}{j! \cdot k! \cdot (n-j-k)} \right)^2$$

Let $\left[\frac{n}{k}\right]$ denote the nearest integer to $\frac{n}{k}$. Then we have that $\frac{n!}{j! \cdot k! \cdot (n-j-k)!}$ achieves its maximum at $j = k = \left[\frac{n}{3}\right]$. This is analogous to the fact that the central binomial coefficient is the largest.

Using this, we can say that

$$\frac{n!}{j! \cdot k! \cdot (n-j-k)!} \leq \frac{n!}{\left[\frac{n}{3}\right]! \cdot \left[\frac{n}{3}\right]! \cdot \left[\frac{n}{3}\right]!} = \frac{n!}{\left(\left[\frac{n}{3}\right]!\right)^3}$$

Plugging this in, we can see that

$$u_{2n} \leq \frac{1}{2^{2n}} \binom{2n}{n} \frac{1}{3^n} \frac{n!}{\left(\left[\frac{n}{3}\right]!\right)^3} \sum_{\substack{j,k \geq 0 \\ j+k \leq n}} \left( \frac{1}{3^n} \frac{n!}{j! \cdot k! \cdot (n-j-k)} \right)$$

This last summation term is just 1, so we have

$$u_{2n} \leq \frac{1}{2^{2n}} \binom{2n}{n} \frac{1}{3^n} \frac{n!}{\left(\left[\frac{n}{3}\right]!\right)^3} = \frac{1}{2^{2n}3^n} \frac{(2n)!}{n!\left(\left[\frac{n}{3}\right]!\right)^3}$$

And using Stirling's approximation,

$$\frac{1}{2^{2n}3^n} \frac{(2n)!}{n!\left(\left[\frac{n}{3}\right]!\right)^3} \approx \frac{\sqrt{2}}{\left(\sqrt{\frac{2\pi}{3}}\right)^3 n^{\frac{3}{2}}}$$

So we have that

$$\sum_{n=1}^{\infty} u_{2n} \leq K \sum_{n=1}^{\infty} \frac{1}{n^{\frac{3}{2}}} < \infty$$

for some appropriate choice of constant $K$. Since this sum is finite, we do not expect to revisit the origin infinitely often with probability 1.

**Theorem.** *(Pólya)*

*The symmetric simple random walk on $\mathbb{Z}^d$ is recurrent if $d = 1$ or $d = 2$ and transient if $d \geq 3$.*

*Proof.* We can give a proof for $d = 4, 5 \ldots$ by following the proof for $d = 3$ above and making some modifications. Alternatively, we can fix a $\mathbb{Z}^3 \subset \mathbb{Z}^d$ and observe that if the walk is recurrent in $\mathbb{Z}^d$ it must also be recurrent in the subspace $\mathbb{Z}^3$. We can restrict the random walk to that subspace by modding out the steps along dimensions not in our $\mathbb{Z}^3$ subspace, and this walk is a simple symmetric random on with respect to $\mathbb{Z}^3$, hence it is not recurrent. Inductively, we can see that such walks cannot be recurrent on any $\mathbb{Z}^d$ for $d \geq 3$. □

It turns out that the probability of a walk returning to the origin is around .35, so the expected number of returns is around .53. Not minuscule, but also certainly not probability 1 and an infinite number of returns.

**Definition.** A **probability measure** on a group $\Gamma$ is a function $p : \Gamma \to [0, 1]$ such that $\sum_{\gamma \in \Gamma} p(\gamma) = 1$.

**Definition.** A probability measure $p$ is **symmetric** if $p(\gamma) = p(\gamma^{-1})$.

**Definition.** The **support** of a probability measure $p$ on a set $X$ is the set of $x \in \mathbb{X}$ such that $p(x) \neq 0$.

**Definition.** A **left-invariant walk** is one in which a walker at some point $\gamma_1$ moves to $\gamma_2$ in one step with probability equal to $p(\gamma_1^{-1}\gamma_2)$ where $p$ is a probability measure on $\Gamma$.

Here's an interesting theorem, which is too hard for us to prove right now:

**Theorem.** *(Varopolous)*

*If $p$ is a symmetric probability measure on a group $\Gamma$ and the support of $p$ is a finite set of elements which generate $\Gamma$ and the random walk associated with $p$ is recurrent, then either $\Gamma$ is finite, $\Gamma$ has a subgroup of finite index isomorphic to $\mathbb{Z}$, or $\Gamma$ has a subgroup of finite index isomorphic to $\mathbb{Z}^2$.*

**Exercise** (5 (i))**.** We wish to show that the walk on $\mathbb{Z}$ is recurrent. Let $\pi(k)$ denote the probability that a random walker starting at some point $k \in \mathbb{Z}$ will eventually reach the origin. We know that $\pi(0) = 1$. Next, observe that $\pi(k) = \frac{1}{2}\pi(k-1) + \frac{1}{2}\pi(k+1)$, as if the walker is at point $k$, then with probability .5 she moves to $k+1$ and with probability .5 to $k-1$. Then the probability that she reaches the origin from $k$ is the sum of half the probability she does so from $k+1$ and half the probability she does so from $k-1$. Thus $\pi(x)$ is a linear function, and since it passes through $\pi(0) = 1$ and is always non-negative, we must have that $\pi(k) = 1$, which implies that from any point, the probability of returning to the origin eventually is 1, hence the walk is recurrent.

**Exercise** (5 (ii))**.** Let $\pi(i,k)$ denote the probability that the walker eventually reaches position $k$ from position $i$. Assume without loss of generality that the first step in the walk is in the positive direction. Note that $\pi = \pi(i, i-1)$, $\pi(i,i) = 1$, and $\pi(i, i-k) = \pi(i, i-j)\pi(i-j, i-k)$. In words, the probability of returning to the origin is exactly the probability of returning from position 1, as we assume that the walker moves to position 1 in the first step, the probability of reaching any point from that same point is clearly 1, and the probability of reaching some position $k$ steps away is the product of that of reaching some position $j$ steps away, then moving from that position to the one that is $k$ steps away.

Now, we have

$$\pi = \pi(1,0) = \frac{1}{2} + \pi(2,0) = \frac{1}{2} + \frac{1}{2}\pi(2,1)\pi(1,0) = \frac{1}{2} + \frac{1}{2}\pi(\pi(3,1) + \frac{1}{2}) = \frac{1}{2} + \frac{1}{4}\pi + \dots$$

This series equals $\frac{1}{2-\pi}$, and setting $\pi = \frac{1}{2-\pi}$, some algebraic manipulation gives us $\pi = 1$, as desired. Hence the walk is recurrent.

**Exercise** (6 (i))**.** We can think of the random walk on $\mathbb{Z}^2$ as the projection of two independent random walks along the orthogonal diagonals. A step in $\mathbb{Z}^2$ is the product of two one-dimensional steps along these lines, so the probability of being at the origin is the product of the probabilities of being at the origin in the two one-dimensional spaces.

**Exercise** (6 (ii))**.** We want to show that if $a < b$, then $a! \cdot b! \geq (a+1)! \cdot (b-1)!$.

We simply divide the both sides by $(b-1)!$ and $a!$ to get $b \geq a$, and we're done.

**Exercise** (7 (i))**.** Suppose the walker on $\mathbb{N}$ is at 0 at time 0 and 1 at time 1. If at time $n \geq 1$ he is at 0, he stays there at time $n+1$. Otherwise, he moves left or right with equal probability. Denote $P_k^n$ the probability that the walker is at position $k$ at time $n$ and $P_k(z) = \sum_{n=0}^{\infty} P_k^n z^n$ the generating function of the sequence $P_k^n$.

We want to compute $P_k^n$ for $n \leq 5$ (the book says for $n \leq 10$ but this is tedious...):

$$P_0^0 = 1 \qquad \begin{matrix} P_0^1 = 0 \\ P_1^1 = 1 \end{matrix} \qquad \begin{matrix} P_0^2 = .5 \\ P_1^2 = 0 \\ P_2^2 = .5 \end{matrix}$$

$$
\begin{aligned}
P_0^3 &= .5 \\
P_1^3 &= .25 \\
P_2^3 &= 0 \\
P_3^3 &= .25
\end{aligned}
\qquad
\begin{aligned}
P_0^4 &= \frac{5}{8} \\
P_1^4 &= 0 \\
P_2^4 &= .25 \\
P_3^4 &= 0 \\
P_4^4 &= \frac{1}{8}
\end{aligned}
\qquad
\begin{aligned}
P_0^5 &= \frac{5}{8} \\
P_1^5 &= \frac{1}{8} \\
P_2^5 &= 0 \\
P_3^5 &= \frac{3}{16} \\
P_4^5 &= 0 \\
P_5^5 &= \frac{1}{16}
\end{aligned}
$$

**Exercise** (7 (ii))**.** To see that $P_0(z) = 1 + z(P_0(z) - 1) + \frac{z}{2}P_1(z)$ think of all of the ways to end up at $k = 0$. The $\frac{z}{2}P_1(z)$ term is half of the probability of being at $k = 1$, which is the probability of moving from $k = 1$ to $k = 0$. The first term represents the probability that we were at $k = 0$ in the previous step, and since $k = 0$ is absorbing, we just add this on.

To see that $P_1(z) = z(1 + \frac{1}{2}P_2(z))$, just observe that the only way to end up at $k = 1$ is to move there from $k = 2$, which occurs with probability equal to half of the probability of being in $k = 2$ at the previous time step.

To see that $P_k(z) = z(\frac{1}{2}(P_{k-1}z + P_{k+1}(z)))$ for $k \geq 2$, observe that for $k \geq 2$, the only way to end up at position $k$ is to have moved there from $k + 1$ or $k - 1$ in the previous step. Each of these moves happens with probability $\frac{1}{2}$.

**Exercise** (7 (iii))**.** We want to deduce from the previous part that $P_k(z) = 2\left(\frac{1-\sqrt{1-z^2}}{z}\right)^k$ for $k \geq 1$ and that $P_0(z) = 1 + \frac{1-\sqrt{1-z^2}}{1-z}$. This follows from establishing a recurrence relation from the previous three definitions.

**Exercise** (7 (iv))**.**

**Exercise** (7 (v))**.** The expected duration of return is infinite. Using the hint, since the probability of being at $k = 0$ is a sequence which converges to 1 as $n$ grows, we have that the expected duration is just a divergent sum.

# Chapter 2

# Free Products of Groups

**Definition.** A **monoid** is a set $M$ with an operation $\circ$ such that:

1. for all $a, b \in M$, $a \circ b \in M$
2. there exists an $e \in M$ such that for all $a \in M$, $e \circ a = a \circ e = a$
3. the operation $\circ$ is associative

**Definition.** The **free monoid** on a set $A$, also called the **set of words on $A$** is the set $W(A)$ of finite sequences of elements of $A$.

An element of $W(A)$ is typically written $w = a_1 a_2 a_3 \dots a_n$ where each $a_i \in A$.

**Definition.** For a word $w = a_1 a_2 \dots a_n$, $n$ is called the **length** of $w$.

The set $A$ is itself the set of words of length 1.

Let $\Gamma_i$ be a family of groups indexed by $i \in I$. Let $A = \bigsqcup_{i \in I} \Gamma_i$ be the disjoint union of all the $\Gamma_i$. We can define an equivalence relation $\sim$ on $W(A)$ as:

> $we_i w' \sim ww'$. That is, two words are equivalent if we can make one into the other by throwing out identity elements
>
> $wabw' \sim wcw'$ if $a, b, c$ are all in the same group $\Gamma_i$ and $c = ab$. That is, two words are equivalent if we can make one into the other by performing multiplication on adjacent elements which come from the same group.

**Claim.** The quotient $W(A)/\sim$ forms a monoid (actually a group).

In order to turn a monoid into a group, we need to assert the existence of inverses. Since our $W(A)$ is a free monoid on a family of groups, each letter already has an inverse, so we can easily verify that the inverse of the words in the class associated with the word $w = a_1 a_2 \dots a_{n-1} a_n$ is $w^- - 1 = a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1}$ by the shoes-and-socks principle.

**Definition.** This quotient $W(A)/\sim$ forms a group called **the free product** of the groups $\Gamma_i$, which is denoted $*_{i \in I} \Gamma_i$.

**Definition.** A word in $W(A)$ is called **reduced** if none of its letters are the identity in any of the $\Gamma_i$ and for any two adjacent letters $a_i, a_{i+1}$, $a_i$ and $a_{i+1}$ come from different groups. That is, they cannot be multiplied together to form a single letter.

**Claim.** Let $\Gamma_i$ be a family of groups and let $W(A)$, $\sim$, and $*_{i \in I} \Gamma_i = W(A)/\sim$ be as above. Then any element in $W(A)/\sim$ is equivalent to a unique reduced word in $W(A)$.

*Proof.* To see the existence of such a reduced word, let $w = a_1 a_2 \dots$ be some reduced word in $W(A)$, $a$ be a letter from some group, and $aw$ be the word formed by concatenating $a$ and $w$.

Then, set

$$\mathcal{R}(w) = \begin{cases} w & a \text{ is the identity in some } \Gamma_i \\ aa_1a_2\dots & a \text{ is not the identity in any } \Gamma_i \text{ and } a \text{ and } a_1 \text{ come from different } \Gamma_i \\ ba_2a_3\dots & a \text{ and } a_1 \text{ come from the same group } \Gamma_j \text{ and } aa_1 = b \text{ and } b \text{ is not the identiy in } \Gamma_j \\ a_2a_3\dots & a \text{ and } a_1 \text{ come from the same group } \Gamma_j \text{ and } aa_1 = e_j \text{ and } e_j \text{ is the identiy in } \Gamma_j \end{cases}$$

Then $\mathcal{R}(aw)$ is a reduced word and is equivalent to $aw$. By inducting on the length of $w$, we can show that every word is equivalent to some reduced word.

To see uniqueness, for each letter $a$ in $A$, denote the mapping $w \mapsto \mathcal{R}(aw)$ as $T(a)$, which is a function from the set of reduced words into itself. For any word $x = b_1b_2\dots$ in $W(A)$ (reduced or not), call $T(w) = T(b_1)T(b_2)\dots$. For $a, b, c$ in the same group $\Gamma_i$ with $ab = c$, we have that $T(a) = T(b)T(c)$ and that if $e_i$ is the identity element in some group, $T(e_i)$ is the identity map. Therefore, $T(w_1) = T(w_2)$ if and only if $w_1 \sim w_2$. Let $\epsilon$ denote the empty word. For each reduced word $w$, we have that $T(w)\epsilon = w$, so if $w_1$ and $w_2$ are two equivalent reduced words, we have that $T(w_1) = T(w_2)$, so $w_1 = T(w_1)\epsilon = T(w_2)\epsilon = w_2$, so $w_1 = w_2$ and we have uniqueness. □

**Claim.** Pick some $\Gamma_j$ and let $\Gamma$ denote the free product over all of the $\Gamma_i$. Then the canonical homomorphism $\phi : \Gamma_i \to \Gamma$ where $\phi(\gamma) = \gamma$ is injective.

*Proof.* If $\gamma$ is the identity element, then $\phi(\gamma)$ is the empty word. Otherwise, $\phi(\gamma)$ is a one-letter word which is (clearly) reduced and not equivalent to the empty word. Since we have uniqueness of reduced word equivalence, each $\gamma$ maps to a unique element in the free product, and $\phi$ is injective. □

**Definition.** The **free group** over a set $X$ is the free product of copies of $\mathbb{Z}$ indexed by $X$, denoted $F(X)$.

We identify each $x \in X$ with the generator $+1$ in the corresponding copy of $\mathbb{Z}$. We can view $X$ as a subset of the free product and $F(X)$ as the set of reduced words in $X \cup X^{-1}$, where we can reduce words by performing the appropriate multiplication for adjacent letters.

**Definition.** The **rank** of the free group $F(X)$ is the cardinality of $X$.

**Definition.** If $\Gamma$ is a group, a **free subset** of $\Gamma$ is an $X \subset \Gamma$ such that the extension of the inclusion $X \hookrightarrow F(X)$ is an isomorphism between the subgroup of $\Gamma$ generated by $X$ onto $F(X)$.

**Example.** The fundamental group of a wedge of $k$ circles is the free group of rank $k$.

**Theorem.** *(The Universal Property of Free Groups)*

*Let $\Gamma$ be a group and $(\Gamma_i)_{i\in I}$ a family of groups indexed by $I$. Next, let $(h_i : \Gamma_i \to \Gamma)_{i\in I}$ be a family of homomorphisms indexed by $I$ such that $h_i$ is a homomorphism from $\Gamma_i$ into $\Gamma$. Then there exists a unique homomorphism $h$ such that for each $\Gamma_j$, applying $h_j$ is equivalent to taking $\Gamma_j$ to the free product $*_{i\in I}\Gamma_i$ and applying $h$.*

*That is, if $\Gamma$ is a group and $X$ a set, and $\phi : X \to \Gamma$ is any function, there exists a unique homomorphism $\Phi : F(X) \to \Gamma$ such that $\phi(x) = \Phi(x)$ for all $x \in X$.*

*Proof.* Let $w = a_1a_2a_3\dots$ be a reduced word in the free product of the $\Gamma_i$ and let $a_{i_j}$ denote that letter $i$ comes from group $\Gamma_j$. Then let $h(w) = h_i(a_{1_i})h_j(a_{2_j})\dots$ where we define $h(w)$ to be the corresponding homomorphism from the group that each letter comes from.

This defines $h$ uniquely in terms of the $h_i$, so given some family of homomorphisms $h_i$ there is a unique homomorphism $h$ satisfying this relationship. □

Let $X$ and $Y$ be two sets. This universal property tells us that any mapping $X \to Y$ has a canonical extension to a group homomorphism $F(X) \to F(Y)$. In particular, if the mapping $X \to Y$ is bijective, the extension is a group isomorphism between $F(X)$ and $F(Y)$.

**Corollary.** *Any group can be realized as the quotient of a free group.*

*Proof.* A group $\Gamma$ can be thought of, in particular, as a set, and we can consider $\Gamma$ as a group a quotient of $F(\Gamma)$ where the relations of $\Gamma$ are the kernel of the quotient map.

□

**Exercise** (7 (Universal Property of Free Monoids))**.** The universal property of free monoids is almost identical to that of free groups. Let $A$ be a set and $W(A)$ the free monoid on that set. Then for any monoid $M$ and a map $f : A \to M$, there exists a unique monoid homomorphism $\phi : W(A) \to M$ which satisfies the property that applying $f$ to some element of $A$ is equivalent to first realizing that element as a letter in $W(A)$ then applying $\phi$ to that letter.

*Proof.* Let $w = a_1 a_2 \dots a_n$ be a word in $W(A)$. Then $\phi(w) = f(a_1)f(a_2)\dots f(a_n)$ so $\phi$ is defined as an application of $f$ to each letter, which uniquely determines $\phi$ with respect to some $\alpha$.

□

Consequently, if $X$ and $Y$ are sets of equal cardinality, there is a monoid isomorphism between $W(X)$ and $W(Y)$ which can be built from any bijection $X \to Y$.

**Exercise** (8)**.** A submonoid of a free monoid need not be free (unlike subgroups of free groups).

**Exercise** (9)**.** We wish to show that the generating function of the free monoid on a finite set of size $k$, corresponding to the number of words of a given length is rational.

*Proof.* Recall that a sequence has a rational generating function if and only if it is a finite linear recurrence. The free monoid has 1 word of length 0, and $k$ words of length 1. To make a word of length $n+1$, we take a word of length $n$ and add one more letter to it, which has recurrence $f(n+1) = kf(n)$.

The $n$th term in the sequence is $k^n$, if we wanted a closed-form expression.

□

**Exercise** (10)**.** We wish to show that two free groups are isomorphic if and only if they have the same rank.

*Proof.* One direction is easy. We have from the universal property that if we have two sets of equal cardinality, the free groups on those sets are isomorphic. Since the rank of a free group is precisely the cardinality of the underlying set, we have that two free groups having the same rank implies they are isomorphic.

Now assume that we have two free groups $F, G$ which are isomorphic. We will show they have the same rank. Since these groups are isomorphic, the size of the set of homomorphisms between $F$ and $\mathbb{Z}_2$ is the same as the size of the set of homomorphisms between $G$ and $\mathbb{Z}_2$. Observe that for a group of rank $r$, there are $2^r$ such homomorphisms, as we can just identify each one with some function from the underlying set into $\mathbb{Z}_2$ and use the universal property to extend that map to a

homomorphism. If $r, s$ are the ranks of $F, G$, we have that $2^r = |\hom(F, \mathbb{Z}_2)| = |\hom(G, \mathbb{Z}_2)| = 2^s$, hence $r = s$.

□

**Exercise** (13)**.** We wish to show that the center of a free group of rank at least 2 where none of the factors are trivial is trivial.

*Proof.* Assume, for the sake of contradiction, that such a free group has an element in its center $w$, and assume that $w$ is reduced and that its first letter is $a$. Then the word $bw$, where $b$ comes from a different group as $a$ is not the same as $wb$, as the reduced word for $bw$ starts with $b$ and the reduced word for $wb$ starts with $a$. Hence $w$ does not commute with $b$ and it is not in the center.

□