Dillan Marroquin
MATH 331.1001
Scribing Week 5
Due. 27 September 2021

Lecture 11

Finitely Generated Groups

Motivation: In linear algebra, to describe every vector in $\mathbb{R}^2$, you only need 2 basis vectors along with a scalar (e.g. we can write $\begin{bmatrix} a \\ b \end{bmatrix} = a\begin{bmatrix} 1 \\ 0 \end{bmatrix} + b\begin{bmatrix} 0 \\ 1 \end{bmatrix} = a\vec{e_1} + b\vec{e_2}$.

For a group G, we can sometimes find a finite subset $\{x_2, \dots, x_n\} \subseteq G$ such that $\forall g \in G$, $\exists \{x_{i_1}, \dots, x_{i_k}\} \subseteq \{x_1, \dots, x_n\}$ and $n_1, \dots, n_k \in \mathbb{Z}$ such that $g = x_{i_1}^{n_1} x_{i_2}^{n_2} \cdots x_{i_k}^{n_k}$.
In this case, we say G is **finitely generated** and that $\{x_1, \dots, x_n\}$ is a set of **generators** of G and we write $G = \langle x_1, \dots, x_n \rangle$.

If G is Abelian and we're using additive notation, then we write elements of $G = \langle x_1, \dots, x_n \rangle$ as $g = n_1 x_{i_1} + \cdots + n_k x_{i_k}$.

WARNING: The analogy between bases for a vector space and generators for a group is not perfect. Notions of linear independence, scalar multiples, and dimension do not make sense for groups in general.

Examples of Finitely Generated Groups

1. The abstract cyclic group of order 2: $G = \{e, \tau\}$ is finitely generated.
   We have $G = \langle \tau \rangle$ because $\tau = \tau^1$ and $e = \tau^0 = \tau^2$.
2. The Klein 4-group $V = \{e, a, b, c\}$ is finitely generated.
   We have $G = \langle a, b \rangle$ because $e = a^0 = b^0$, $a = a^1$, $b = b^1$, and $c = a^1 b^1$.
3. Any finite group G is finitely generated because $G = \langle G \rangle$.

Remark. If $|G| = \infty$, then it can be finitely generated.

4. The group $(\mathbb{Z}, +, 0)$ is finitely generated.
   We have $\mathbb{Z} = \langle 1 \rangle$ because $\forall n \in \mathbb{Z}$, $n = n \cdot 1$. (Note that $\mathbb{Z} = \langle -1 \rangle$ also!)
5. The group $\mathbb{Z}/n$ is finitely generated.
   Just like for $\mathbb{Z}$, we have $\mathbb{Z}/n = \langle [1] \rangle$.

Proposition (11.1)**.** Let $n > 1$. Then $\mathbb{Z}/n = \langle [a] \rangle$ iff $\gcd(a, n) = 1$. Particularly, the elements of the group of units $(\mathbb{Z}/n)^\times$ are precisely the set of all possible generators!

Example (Non-Abelian Example)**.** Let $S_3 := \{f : 1,2,3 \to 1,2,3 | f \text{ is bijective}\}$ where the group operation is function composition. We can write $f \in S_3$ as a table:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$$

with the 6 elements of S_3 being:

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

One can check that $S_3 = \langle \sigma, \tau \rangle$, where $\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ and $\tau = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$.
Indeed, $S_3 = \{e = \sigma^0 \tau^0, \sigma, \sigma^2, \tau, \sigma \circ \tau, \sigma^2 \circ \tau\}$.

Example (Non-Example)**.** Any group that is not finitely generated must be infinite.

Proposition (11.2)**.** The group $(\mathbb{Q}, +, 0)$ is NOT finitely generated.

Lecture 12

Cyclic Groups

i.e. groups that can be generated by 1 element.

Lemma (12.1)**.**

1. Let G be a subgroup and $a \in G$. Then $\forall k, l \in \mathbb{Z}$, $a^k \cdot a^l = a^{k+l}$.

2. Let $(G, +, 0)$ be an Abelian group and let $a \in G$. Then

   i. $\forall k, l \in \mathbb{Z}$, $ka + la = (k+l)a$ and

   ii. $\forall k, l \in \mathbb{Z}$, $l(ka) = lka$.

Proposition (12.2)**.** Let G be a group and $a \in G$.

1. The subset $\langle a \rangle := \{a^k | k \in \mathbb{Z}\} = \{\ldots, a^{-1}, a^0, a^1, \ldots\}$ is a subgroup of G called the **cyclic subgroup** generated by a.

2. If $H \leq G$ is any subgroup of G containing $a \in H$, then $\langle a \rangle \leq H$. That is, a is the "smallest" subgroup of G containing a.

Definition (12.3)**.** A group is **cyclic** iff $a \in G$ such that $G = \langle a \rangle$.

Examples of Cyclic Groups/Subgroups

1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ is cyclic.

2. Let $n > 1$. $n\mathbb{Z} := \{nk | k \in \mathbb{Z}\} = \langle n \rangle$ is a cyclic subgroup of $\mathbb{Z}$.

3. The trivial group $\{e\} = \langle e \rangle$ is cyclic.

4. The abstract cyclic group $G = \{e, \tau\} = \langle \tau \rangle$ is obviously cyclic.

5. $\mathbb{Z}/n = \langle [1] \rangle$.

6. Let $\mathbb{R}^\times := (\mathbb{R} - \{0\}, \cdot, 1)$. Let $H = \{1, -1\}$. Then $H = \langle 1 \rangle$.

7. Let $\mathbb{C}^\times := (\mathbb{C} - \{0\}, \cdot, 1)$ and let $H = \{1, i, -1, -i\}$. Then $H = \langle i \rangle$.

Definition (12.4)**.** Let G be a group, $a \in G$. The **order of a, $|a|$**, is the smallest positive integer such that $a^n = e$. If no such integer exists, then $|a| = \infty$.

Proposition (12.5)**.** Let G be a group, $a \in G$. If $|a| = n$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. In particular, $|\langle a \rangle| = |a|$.

Corollary (12.6)**.** Let G be a finite group. Then...

1. Every element of G has finite order and

2. $\forall a \in G$, $|a| \,\big|\, |G|$.

Lecture 13

In-class assistance for Problem Set 3; Alex was a big help :)