Group Theory

Lecture 7, Sunday November 27, 2022
Ari Feiglin

7.1 Free Groups

Definition 7.1.1:

A **graph** is an ordered pair $G = (V, E)$ where V is the set of **vertices** and E is the set of **edges**. If G is **ordered** then $E \subseteq V \times V$, and if G is **unordered** then $E \subseteq \mathcal{P}(V)$ where the size of each set in E has at most 2 elements (or exactly 2 if the graph doesn't contain self-loops).

Definition 7.1.2:

An **isomorphism** between two graphs $G = (V, E)$ and $G' = (V', E')$ is a bijective function $\varphi\colon V \longrightarrow V'$ such that $\{u, v\} \in E$ if and only if $\{\varphi(u), \varphi(v)\} \in E'$. An **automorphism** over a graph G is an isomorphism between it and itself. The set of automorphisms over G is denoted $\mathrm{Aut}(G)$.

Notice that if σ, τ are isomorphisms between G_1 and G_2 and G_2 and G_3 then $\tau \circ \sigma$ is an isomorphism between G_1 and G_3, since $\{u, v\} \in E_1$ if and only if $\{\sigma(u), \sigma(v)\} \in E_2$ which is equivalent to $\{\tau \circ \sigma(u), \tau \circ \sigma(v)\} \in E_3$. And if σ is a graph isomorphism, so is σ^{-1} since if $\{u, v\} \in E_2$ then let u' and v' be their preimages and so $\{\sigma(u'), \sigma(v')\} \in E_1$ and therefore $\{u', v'\} = \{\sigma^{-1}(u'), \sigma^{-1}(v')\} \in E_1$ as required. This means that $\mathrm{Aut}(G)$ is a group under composition.
Notice that by definition, an automorphism simply permutes the vertices, so $\mathrm{Aut}(G) \leq S_V$.

Example:

We define a graph $C_n^G = (\mathbb{Z}_n, E)$ where $E = \{\{k, k+1\} \mid k \in \mathbb{Z}_n\}$. Then we define the **dihedral group** to be $D_n = \mathrm{Aut}\left(C_n^G\right) \subseteq S_n$ (really it is a subgroup of the permutations over $\mathbb{Z}_n$).
Notice that C_n^G represents a regular polygon with n vertices, and D_n is the set of all symmetries of a regular polygon with n vertices (it represents all the actions you can do on the polygon without ripping or deforming it, like rotating, flipping, etc). As it turns out, all these operations can be done via a combination of rotating and flipping.
Notice then that if $\sigma \in D_n$ then $\sigma(1) = \sigma(0) + 1$ or $\sigma(0) - 1$, so let $k = \sigma(0)$. If $\sigma(1) = k + 1$ then $\sigma(2) = k + 2$ (since it can't be k since that is $\sigma(1)$), and so on: $\sigma(i) = k + i$. And if $\sigma(1) = k - 1$ then $\sigma(i) = k - i$. So we have n choices for $\sigma(0)$, and then 2 choices for $\sigma(1)$ which together determine the rest of σ. Thus there are $2n$ choices for σ, so $|D_n| = 2n$.
Notice that if we define σ to be a rotation by one, that is $\sigma(k) = k + 1$ and τ to be the flip around 0, that is $\tau(1) = -1 = n - 1$ and in general $\tau(k) = -k$, every element in D_n can be written as either σ^i or $\sigma^i\tau$. So

$$D_n = \left\{\sigma^i, \sigma^i\tau\right\}.$$

The proof of this follows the inuition above, suppose $\pi \in D_n$, then let $k = \pi(0)$, then $\pi(1) = i \pm 1$. If $\pi(1) = k + 1$ then as explained above $\pi(i) = k + i$, so $\pi = \sigma^k$ (since $\sigma^k(i) = k + i$). And if $\pi(1) = k - 1$ then as explained above $\pi(i) = k - i$, and $\sigma^k\tau(i) = \sigma^k(-i) = k - i$.
Notice that $\tau^2 = I$, $\sigma\tau\sigma = I$ and $\tau\sigma^i\tau = \sigma^{-i}$ (intuitively, flipping twice results in the same graph; flipping then rotating then flipping and rotating is as if you rotated, then rotated in the opoosite direction, doing nothing; and flipping then rotating then flipping back is as if you rotated in the opposite direction), so $\tau\sigma^i = \sigma^{-i}\tau$.

Definition 7.1.3:

We define the **free group** over an alphabet $\Sigma = \{x_1, \ldots, x_n\}$ is the Kleene closure of $\Sigma' = \left\{x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}\right\}$. This is denoted $\mathbb{F}_n$. It is a group over the operation of word concatenation. We use the notation $\langle x_1, \ldots, x_k \mid w_1, \ldots, w_t\rangle$ where $w_1, \ldots, w_n \in \mathbb{F}_k$ as the group ${}^{\mathbb{F}_k}\!/_{R}$ where R is the smallest normal subgroup of $\mathbb{F}_k$ which contains all of the w_j. That is $R = \left\langle\left\{gw_jg^{-1} \;\middle|\; g \in \mathbb{F}_k\right\}\right\rangle$.

Notice that $\mathbb{F}_k$ isn't abelian for any $k > 1$ and for $k = 1$, $\mathbb{F}_1 = \langle x\rangle \cong \mathbb{Z}$.

We can define the dihedral group by:

$$D_n = \left\langle \sigma, \tau \mid \sigma^n, \tau^2, \sigma\tau\sigma\tau \right\rangle$$

Similarly:

$$\mathbb{Z}_n = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = \langle x \mid x^n \rangle$$

Since $n\mathbb{Z} = \langle n \rangle = \langle 1^n \rangle$. And

$$\mathbb{Z}_n \times \mathbb{Z}_m = \langle x, y \mid x^n = 1, y^n = 1, xy = yx \rangle$$

This is simply an abuse of notation for $\left\langle x, y \mid x^n, y^n, xyx^{-1}y^{-1} \right\rangle$.
Look at the following group:

$$G = \left\langle x, y \mid x^5 = y^2 = 1, yxy^{-1} = x^3 \right\rangle$$

Then $x = y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^3y^{-1} = (yxy^{-1})^3 = x^9$, so $x = x^9$, so $x^8 = 1$ and $x^5 = 1$ and since 8 and 5 are coprime, $x = 1$. So $G = \left\langle y \mid y^2 = 1 \right\rangle$.
It actually turns out that there does not exist an algorithm which determines whether or not given a representation of a finite group, the group is trivial.

Definition 7.1.4:

The **Quaternion Group** of size $2n$ is the group:

$$Q_{2n} = \left\langle x, y \mid x^n = y^2, yx = yx^{-1}, y^4 = 1 \right\rangle = \left\{ x^iy^j \mid 0 \leq i \leq n-1, 0 \leq j \leq 3 \right\}$$

Lemma 7.1.5:

Every group of prime order is cyclic.

Proof:

Let $e \neq a \in G$ then $o(a) \mid p$, so $o(a) = p$ and therefore $G = \langle a \rangle$.

Theorem 7.1.6:

The following are all the groups of order < 16, up to isomorphism:

1	2	3	4	5	6	7	8
$\{e\}$	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_5$	$\mathbb{Z}_6, S_3$	$\mathbb{Z}_7$	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, Q_4$
9	10	11	12	13	14	15	
$\mathbb{Z}_9$	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_{10}, D_5$	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6, A_4, D_6, Q_6$	$\mathbb{Z}_{13}$	$\mathbb{Z}_{14}, D_7$	$\mathbb{Z}_{15}$	

We will not be proving this.

7.2 Chains

Definition 7.2.1:

A **chain** of groups $(A_1, \dots, A_n)$ are homomorphisms $(f_1, \dots, f_{n-1})$ where $f_i \colon A_i \longrightarrow A_{i+1}$ such that $f_{i+1} \circ f_i = I$ ($\operatorname{Im} f_i \subseteq \operatorname{Ker} f_{i+1}$). And a chain is **exact** if $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$).

Notice that $A \xrightarrow{f} B \longrightarrow \{e\}$ is exact if and only if f is an epimorphism (surjective) and $\{e\} \longrightarrow A \xrightarrow{f} B$ is exact if and only if f is a monomorphism (injective). And so $\{e\} \longrightarrow A \xrightarrow{f} B \longrightarrow \{e\}$ is exact if and only if f is an isomorphism. And $\{e\} \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \{e\}$ is exact if and only if f is an monomorphism and g is an epimorphism and $\operatorname{Im} f = \operatorname{Ker} g$. Since $C \cong {}^{B}\!/_{\operatorname{Ker} g}$ and $\operatorname{Im} f \cong A$, so $\operatorname{Ker} g \cong A$.