10.6. Wednesday for MAT4002

10.6.1. Reviewing On Groups

■ **Example 10.6** Let D_{2n} be the regular polygon P with $2n$ sides in $\mathbb{R}^2$, centered at the origin. It's clear that D_{2n} is **invariant** with $2n$ rotations, or with 2 reflections. Let a denote the rotation of D_{2n} clockwise by degree π/n, and b denote the reflection over lines through the origin.

As a result, $\{e, a, a^2, \dots, a^{n-1}\}$ forms a group; and $\{e, b\}$ forms a group.

Therefore, all elements of D_g can be obtained by $a^i b^j, 0 \le i \le 3, 0 \le j \le 1$.

Any finite operations of rotation (the rotation degree is a multiple of π/n) and reflection can be represented as $a^i b^j$.

Geometrically, we can check that $ba = a^{n-1}b$. ■

Definition 10.14 [Product Group] Let G, H be two groups. The **product group** $(G \times H, *)$ is defined as

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

$$\text{with} \quad (g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

■

For example, $(\mathbb{R} \times \mathbb{R}, +) = \{(x, y) \mid x, y \in \mathbb{R}\}$ coincides with the usual $\mathbb{R}^2$, where

$$(x, y) * (x', y') = (x + x', y + y')$$

Definition 10.15 A map between two groups $\phi : G \to H$ is a **homomorphism** if

$$\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$$

In other words, a homomorphism is a map preserving multiplications of groups. ■

■ **Example 10.7** Let $G = (\mathbb{R}, +, 0)$, and $H = \{H_2, *, I_2\}$, with H_2 of the form

$$H_2 = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in \mathbb{R} \right\}$$

Define a mapping

$$\begin{aligned} \phi : \quad & G \to H \\ \text{with} \quad & x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Then ϕ is a homorphism:

$$\begin{aligned} \phi(x *_{\mathbb{R}} y) &= \phi(x + y) \\ &= \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \\ &= \phi(x) *_{H_2} \phi(y) \end{aligned}$$

■

Definition 10.16 [Isomorphism] A homomorphism $\phi : G \to H$ is an isomorphism if ϕ is bijective. The isomorphism between G and H is denoted as $G \cong H$. ■

Actually, a group can be represented as a Cayley Table:

$$G = \begin{array}{c|cccc} \circ & g_1 & g_2 & \cdots & g_n \\ \hline g_1 & g_1 \circ g_1 & g_1 \circ g_2 & \cdots & g_1 \circ g_n \\ g_2 & g_2 \circ g_1 & g_2 \circ g_2 & \cdots & g_2 \circ g_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g_n & g_n \circ g_1 & g_n \circ g_2 & \cdots & g_n \circ g_n \end{array}, \qquad H = \begin{array}{c|cccc} \circ & h_1 & h_2 & \cdots & h_n \\ \hline h_1 & h_1 \circ h_1 & h_1 \circ h_2 & \cdots & h_1 \circ h_n \\ h_2 & h_2 \circ h_1 & h_2 \circ h_2 & \cdots & h_2 \circ h_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ h_n & h_n \circ h_1 & h_n \circ h_2 & \cdots & h_n \circ h_n \end{array}$$

The groups $G \cong H$ if and only if we can find a bijective $\phi : G \to H$ such that, the Cayley

Table of $(H,\circ)$ can be generated from the Cayley Table of $(G,\circ)$ by replacing each entry of G with its image under ϕ.

10.6.2. Free Groups

Definition 10.17

- Let S be a (finite) set, which is considered as an "alphabet".
- Define another set $S^{-1} := \{x^{-1} \in x \in S\}$. We insist that $S \cap S^{-1} = \emptyset$.
- A **word** in S is a finite sequence $w = w_1 \cdots w_m$, where $m \in \mathbb{N}^+ \cup \{0\}$, and each $w_i = \in \cup S^{-1}$. In particular, when $m = 0$, we view w as the empty sequence, denoted as $\emptyset$.
- The **Concatenation** of two words $x_1 \cdots x_m$ and $y_1 \cdots y_n$ is the word $x_1 \cdots x_m y_1 \cdots y_n$
- Two words w, w' are **equivalent**, denoted as $w \sim w'$, if there are words $w_1, \dots, w_n$ and $w = w_1, w' = w_n$ such that

$$w_i = \cdots y_1 x x^{-1} y_2 \cdots, \qquad w_{i+1} = \cdots y_1 y_2 \cdots$$

or

$$w_i = \cdots y_1 y_2 \cdots, \qquad w_{i+1} = \cdots y_1 x x^{-1} y_2 \cdots$$

for some $x \in S \cup S^{-1}$.

■

■ **Example 10.8** For example, $S = \{a, b\}$ and $S^{-1} = \{a^{-1} b^{-1}\}$ and

$$w = aabab^{-1}b^{-1}a^{-1}abaabb^{-1}a$$
$$w' = aabab^{-1}b^{-1}a^{-1}abaaa$$

Here w and w' differs by bb^{-1}. Therefore, $w \sim w'$, and w is said to be a elementary expansion of w'. ■

R We insist that $(s^{-1})^{-1} = s, \forall s^{-1} \in S^{-1}$, since otherwise for $x = s^{-1} \in S^{-1}$, we cannot define $(s^{-1})^{-1}$.

Moreover, for

$$w = aabab^{-1}b^{-1}a^{-1}abaabb^{-1}a$$
$$w'' = aabab^{-1}b^{-1}baabb^{-1}a,$$

w and w'' differs by $a^{-1}a$, i.e., $a^{-1}(a^{-1})^{-1}$, and therefore $w \sim w''$.

Definition 10.18 [Free Group] The **free group** $F(S)$ is defined to be the equivalence class of words, i.e.,

$$[w] := \{w' \text{ is a word in } S \mid w \sim w'\} \in F(S)$$

R $F(S)$ is indeed a group:

- $[w] * [w'] = [ww']$ (concatenation) check $w_1 \sim w_2, u_1 \sim u_2$ implies $w_1u_1 \sim w_2u_2$
- Identity element: $e = [\emptyset]$
- Inverse element: $[x_1 \cdots x_n]^{-1} = [x_n^{-1} \cdots x_1^{-1}]$

Example 10.9 Let $S = \{a\}$ and $S^{-1} = \{a^{-1}\}$. Any word w has the form

$$w = a \cdots aa^{-1} \cdots a^{-1}a \cdots aa^{-1} \cdots a^{-1} \cdots$$

In shorthand, we denote w as $w = \cdots a^p(a^{-1})^q a^r (a^{-1})^s \cdots$, and

$$\begin{aligned}[w] = [\cdots a^p(a^{-1})^q a^r (a^{-1})^s \cdots] &= [\cdots a^{p-1}(a^{-1})^{q-1} a^r (a^{-1})^s \cdots] \\ &= [\cdots a^{p-1}(a^{-1})^{q-2} a^{r-1} (a^{-1})^s \cdots],\end{aligned}$$

e.g., we can always eliminate the adjacent terms a and a^{-1} up to equivalence class. Therefore, $F(S) = \{\cdots, [a^{-2}], [a^{-1}], [\emptyset], [a], [a^2], \cdots\}$.

It's clear that $F(S) \cong \mathbb{Z}$, where the isomorphism $\phi : \mathbb{Z} \to F(S)$ is $\phi(n) = [a^n]$.

Example 10.10 Let $S = \{a, b\}$ and $S^{-1} = \{a^{-1}, b^{-1}\}$. In this case, $[ab] \neq [ba]$, and $[ab^{-1}a^2b^2a^{-2}b]$ cannot be reduced further.

Since S is not an abelian group in such case, we imply $F(S) \ncong \mathbb{Z} \times \mathbb{Z}$.

10.6.3. Relations on Free Groups

Definition 10.19 [Group With Relations] Let S be a set. A **group with relations** is written as

$$G =< S \mid R(S) >$$

where

- $R(S)$ consists of elements in $F(S)$
- Every element in G can be written as the form $[w] \in F(S)$, and we insist that $[w] = [w']$ in G if
  - w and w' differ by some $xx^{-1}, x \in S \cup S^{-1}$, or
  - w and w' differ by some element $z \in R(S)$, or its inverse.

Example 10.11 Let $G = \langle a, b \mid a^2, b^2, abab^{-1}a^{-1}b^{-1} \rangle$, we want to enumerate all possible elements in G. Obseve that

$$[b^{-1}] = [b^{-1}b^2] = [b], \quad \text{similarly } [a^{-1}] = [a]$$

$$[bab] = [abab^{-1}a^{-1}b^{-1}bab] = [abab^{-1}b] = [aba]$$

As a result,

- $[a^{-n}] = [a^n]$ and $[b^{-n}] = [b^n]$

- $[a^{2n+1}] = [a], [b^{2n+1}] = [b], [a^{2n}] = [\emptyset], [b^{2n}] = [\emptyset]$

- For another type of element of G, it must be of the form $[\cdot abababab \cdots]$.

  Each aba can be changed into bab, and finally it will be reduced into the form $[ab]$.

Therefore, the elements in G are

$$[\emptyset], [a], [b], [ab], [ba], [aba]$$

In fact, $G \cong S_3$. ▪