1.2 Dihedral Groups

Recall

\[ D_6 \text{ group of symmetries of } \Delta \]

\[ \begin{align*}
1 & \rightarrow r & \rightarrow 1 \\
1 & \rightarrow s & \rightarrow 1 \\
r^2 & \rightarrow r^{-1} & \\
s^2 & \rightarrow s^{-1} & \\
rs & \rightarrow sr^{-1} & \\
rs & \rightarrow r^{-1}s &
\end{align*} \]

Elements

\[ r^3 = s^2 = 1 \]

\[ rs = sr \]

That is, \( D_6 \) is completely determined by the relations

\[ r^3 = s^2 = 1 \quad rs = sr \]

We give a presentation of \( D_6 \) in terms of generators and relations as

\[ \langle r, s \mid r^3 = s^2 = 1, \; rs = sr^{-1} \rangle \]

uniqueness issues

\[ \langle x, y \mid x^2 = y^3 \rangle \]

\[ \langle x, y \mid x^2 = y^3 = 1 \rangle \]

"\( D_6 \) is a homomorphic image of free groups"

More General Dihedral Groups

The symmetries of a regular \( n \)-gon are given by relations

\[ \begin{align*}
& \langle 1 \rangle \quad \text{and reflections} \quad \text{which reverse the order of numerical notation} \\
& \langle 1 \rangle \quad \text{and} \quad \text{rotations} \\
& \text{There are exactly } n \text{ symmetries of an } n \text{-gon}
\end{align*} \]
For a regular \( n \)-gon, let
\[
\begin{align*}
T &= \text{clockwise rotation by } \frac{2\pi}{n} \\
S &= \text{reflection through line through position one and the center}
\end{align*}
\]
It can be shown that the group of symmetries of the regular \( n \)-gon has presentation
\[
\langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle
\]
\text{Axon: } |D_{2n}| = 2n
\begin{align*}
|r| &= n \\
|s| &= 2
\end{align*}
\text{N.B. } D_{2n} \text{ is not abelian for } n \geq 3
\text{The proof is left.}

\section{Symmetric Groups}
Let \( \Omega \) be a nonempty set and let \( S_\Omega \) be the set of bijections of \( \Omega \) to itself. Then \( S_\Omega \) is a group, \( o^2 = e \) and
\[
o^{-1} \text{ is the inverse function } o^{-1}(x) \rightarrow x
\]
Refer to elements of \( S_\Omega \) as \textit{permutations} of \( \Omega \)
For \( \Omega = \{1, 2, \ldots, n\} \) we use \( S_n \) to denote \( S_\Omega \) for \( n \geq 1 \)
\text{Cycles in } S_n

\text{Example: } (3\,6\,19) \in S_n
\text{the mean the permutation of } \{1, 2, 3, \ldots, n\} \text{ st.}
\[
\sigma(x) = \begin{cases} 
3 & x = 9 \\
6 & x = 3 \\
19 & x = 6 \\
& x = 1 
\end{cases}
\]
\text{N.B. } (3\,9\,16) = (6\,19\,3) = (19\,6\,3) = (9\,3\,1)
In general \((a_1, a_2, \ldots, a_m)\) for \(m \geq 1\) and distinct positive integers \(a_1, a_2, \ldots, a_m\) all \(\leq n\) we have permutation

\[
\begin{align*}
  a_1 & \mapsto a_2 \\
  a_2 & \mapsto a_3 \\
  & \quad \quad \quad \quad \quad \quad \\
  a_m & \mapsto a_n \\
  a_n & \mapsto a_1
\end{align*}
\]

We say the \textit{length} of a cycle is \(m\).

We may call this an \(m\)-\textit{cycle}.

NB. cycles of length 1 are trivial, identity permutations and are typically called.

\textbf{Def:} \ Two cycles \((a_1, \ldots, a_m)\) and \((b_1, \ldots, b_m)\) are disjoint if

\[
\{a_1, \ldots, a_m\} \cap \{b_1, \ldots, b_m\} = \emptyset
\]

\textbf{Cycle decomposition}

\textbf{Example:} \ \(\sigma \in S_7\)

\[
\begin{align*}
  1 & \mapsto 3 \\
  2 & \mapsto 5 \\
  3 & \mapsto 4 \\
  4 & \mapsto 1 \\
  5 & \mapsto 7 \\
  6 & \mapsto 6 \\
  7 & \mapsto 2
\end{align*}
\]

We have written \(\sigma\) as a product of disjoint cycles.

We say that this is a \textit{cycle decomposition} of \(\sigma\).
Prop: For \( n \geq 1 \) every permutation in \( S_n \) can be written as a disjoint product of cycles, unique up to the ordering of the cycles.

Proof (omitted — in detail)

Remarks

1. Re: uniqueness

\[(134)(257) = (257)(134) = (572)(413)\]

"is" unique decomposition

2. Disjoint cycles commute (Exercise)

3. \((13)(24) \neq (24)(13) !!!\)

So \( S_n \) is not abelian for \( n \geq 3 \)

4. Given \( \sigma \in S_n \), the order of \( \sigma \) is the least common multiple of the lengths of the cycles in its disjoint composition.

N.B. in particular the order of an \( n \)-cycle is \( n \).

All of these are Exercises

5. \(|S_n| = n!|\)
§1.4 MATRIX GROUPS

Assume that \( F \) is an additive abelian group with identity \( 0 \) and \( F \setminus \{0\} \) is equipped with a multiplicative abelian group identity \( 1 \) such that \( a(b+c) = ab + ac \), i.e., is distributive.

We say \( F \) is a FIELD and \( F \setminus \{0\} \) a multiplicative group denoted \( F^\times \).

**E.g.:** \( \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z} \), \( p \) prime.

Next let \( n \) be a positive integer and \( F \) a field.

\( M_n(F) \) denotes the set of \( n \times n \) matrices with entries from \( F \) where matrix arithmetic proceeds as usual.

Set \( GL_n(F) \) to be the set of all matrices in \( M_n(F) \) with nonzero determinant

\[ \{ A \in M_n(F) \mid \det A \neq 0 \} \]

then this is a multiplicative group with identity \( \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \).

Under matrix multiplication, group inverses are simply matrix inverses.

**Comment:** For \( n > 1 \), \( GL_n(F) \) is non-abelian.

§1.5 QUATERNIONS

The permutation group \( \mathbb{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\} \) has multiplication

\[ ii = jj = kk = -1, \quad Ri = j, \quad ik = -j \]

\[ ij = k, \quad ji = -k, \quad (-1)(-1) = 1 \]

and for all \( a \in \mathbb{Q}_8 \)

\[ a = a_{(-1)} = -a \]
§ 1.6 HOMOMORPHISMS

**Def** Let \((G, \cdot)\) and \((H, \circ)\) be groups and let \(\varphi: G \rightarrow H\) be a map such that

\[
\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)
\]

\[
(a, b) \xrightarrow{\alpha} a \cdot b \\
G \times G \xrightarrow{\varphi} G \\
H \times H \xrightarrow{\circ} H
\]

**Example** Recall \(D_{2n}\)

\(\sigma\) maps \(i\) to position \(j\)

Write \(\rho_\sigma(i) = j\) is \(\sigma\) viewed as a permutation in \(S_n\)

Then \(\Phi_n: D_{2n} \rightarrow S_n\)

\[
\sigma \mapsto \rho_\sigma
\]

is a homomorphism

Then \(\Phi_n\) is an **injective** homomorphism i.e. 1-1 i.e. a **MONOMORPHISM** (it is surjective only for \(D_6\))

Consider \(n = 3\)

\(|D_6| = |S_3| = 6\) so \(\Phi_3\) is bijective, hence surjective

**Def** A group homomorphism \(\varphi: G \rightarrow H\) is an **ISOMORPHISM** if it is bijective

We will generally consider isomorphic groups "the same"
Examples

Let \( \Omega, \Omega' \) be nonempty sets of the same cardinality.

Then \( \Sigma_\Omega = \Sigma_{\Omega'} \)

Proof: Exercise

Let \( B \) be bijection between sets

\[ \sigma(B(n)) \]

Let \( n \) be an integer \( \geq 2 \), let \( F \) be a field, and let \( \sigma \in S_n \). Consider the matrix \( \Theta(\sigma) \) with

1 in the \( i \)-th column, \( 0 \)s in the row, for \( 1 \leq i \leq n \) and

0 elsewhere.

\[
\begin{pmatrix}
1 & 2 & 3 \\
3 & 1 & 2
\end{pmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{bmatrix}
\]

(Deck!

Then for all \( n \geq 2 \) the map

\[
\Sigma_n \rightarrow GL_n(F)
\]

\( \sigma \mapsto \Theta(\sigma) \)

is well-defined and a group homomorphism. (Exercise)

N.T.S. \( \Theta(\sigma) \) is invertible.