Math 3500

Algebra I: Group Theory

Book 2

Similar to HW#2: How many elements of each order does S_4 have?

1 element of order 1 : $()$ = identity

9 elements of order 2 : $(12), (13), (14), (23), (24), (34),$ ← $\binom{4}{2} = 6$ transpositions

$(12)(34), (13)(24), (14)(23)$ ← $\frac{1}{2!}\binom{4}{2}\binom{2}{2} = \frac{6}{2} = 3$

8 elements of order 3: $(123), (124), (132), (134), (142), (143), (234), (243)$

6 elements of order 4: $(1234), (1243), (1324), (1342), (1423), (1432)$

$24 = 4! = |S_4|$ $\qquad |S_n| = n! = 1 \times 2 \times 3 \times \cdots \times n$

In S_n the number of n-cycles is $(n-1)!$

The binomial coefficient $\binom{n}{k}$ ("n choose k") is the number of ways to choose a subset of size k from a set of size n.

By the way, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

$\binom{n}{k}$ = k^{th} entry in n^{th} row of Pascal's Triangle

Binomial Theorem $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

$\binom{4}{2}$ = number of 2-subsets in $[4] = \{1,2,3,4\}$
$= 6$

Pascal's Triangle

n=0	1							
n=1	1	1						
n=2	1	2	1					
n=3	1	3	3	1				
n=4	1	4	6	4	1			
n=5	1	5	10	10	5	1		
n=6	1	6	15	20	15	6	1	
n=7	1	7	21	35	35	21	7	1

k=0, k=1, k=2, k=3, k=4, k=5, k=6, k=7

A <u>transposition</u> is a 2-cycle $(i\ j) \in S_n$, $i \neq j$ in $[n] = \{1, 2, \cdots, n\}$.

Products of disjoint transpositions e.g. $(1\ 3)(2\ 5)(6\ 8) \in S_8$ are elements of order 2.

How many elements of order 2 are there in S_7?

Transpositions: $(12), (13), (14), \cdots, (67)$ i.e. $(i\ j)$ where $i \neq j$ in $[7] = \{1, 2, \cdots, 7\}$

$\binom{7}{2} = 21$ transpositions

Products of two disjoint transpositions e.g. $(26)(34) = (3\ 4)(2\ 6)$

Number of these is $\frac{1}{2}\underbrace{\binom{7}{2}}_{21}\underbrace{\binom{5}{2}}_{10} = 105$.

Products of three disjoint transpositions eg. $(1\ 5)(27)(36) = (15)(36)(27) = (27)(15)(36) = \cdots$

Number of these is $\underbrace{\frac{1}{3!}}_{\frac{1}{6}}\underbrace{\binom{7}{2}}_{21}\underbrace{\binom{5}{2}}_{10}\underbrace{\binom{3}{2}}_{3} = \frac{21 \times 10 \times \cancel{3}}{\cancel{6}\,2} = 105$

Number of 3-cycles in S_7 eg. (274): $2\binom{7}{3} = 2 \times 35 = 70$

Number of products of two disjoint 3-cycles: eg. $(274)(356) = (356)(274)$

$\cancel{\tfrac{1}{2}} \cdot 70 \cdot \binom{4}{3} \cdot \cancel{2} = 70 \cdot 4 = 280$

$280 + 70 = 350$ elements of order 3 in S_7

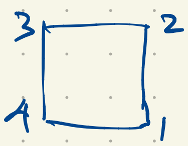
Elements of order 12 in S_7 eg. $(1\ 4\ 2)(3\ 7\ 5\ 6)$

$70 \cdot 3! = 70 \cdot 6 = 420$ elements of order 12 in S_7.

Revisiting the dihedral group of order 8 (symmetry group of a square)

$G = \{ I, R, R^2, R^3, D, D', V, H \}$

viewed as a group of permutations of the four vertices



$I \longmapsto ()$

$R \longmapsto (1234)$

$R^2 \longmapsto (13)(24)$

$R^3 \longmapsto (1432)$

$H \longmapsto (12)(34)$

$V \longmapsto (14)(23)$

$D \longmapsto (13)$

$D' \longmapsto (24)$

$G \cong$ subgroup of S_4: $\{(), (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$

$= \langle (1234), (13) \rangle$

$RV = (1234)(14)(23) = (24) = D'$

This is an example of a <u>permutation group</u> of degree 4, i.e. a subgroup of S_4.

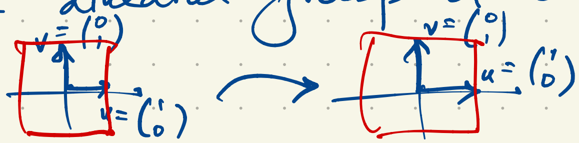
A <u>permutation group</u> of degree n is a subgroup of the symmetric group S_n.

<u>Theorem</u> (Cayley's Representation Theorem) Every finite group is isomorphic to a permutation group. In fact, if $|G| = n$ then G is isomorphic to a subgroup of S_n. (But we can usually do better. Eg. the dihedral group of order 8 is isomorphic to a subgroup of S_8. But S_4 is even better.)

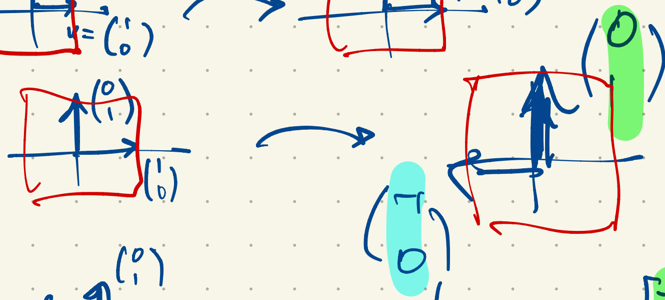
The two most important general classes of examples of groups are (i) <u>permutation groups</u> (i.e. subgroups of S_n) and

(ii) <u>linear groups</u> (i.e. subgroups of $GL_n(F) = \{$invertible $n \times n$ matrices over a field $F\}$). eg. $F = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ (integers mod p)

The dihedral group of order 8 is also a subgroup of $GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\}$.

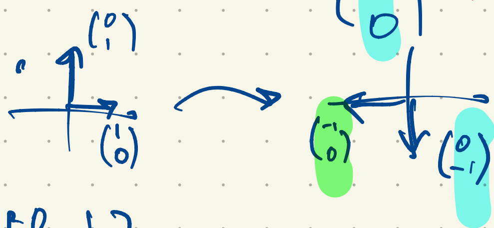
I:  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$

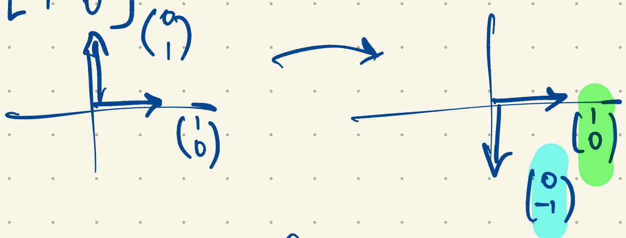
R:  $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -y \\ x \end{bmatrix}$$

(the vector $\begin{bmatrix} x \\ y \end{bmatrix}$ rotated 90° counter-clockwise about the origin)

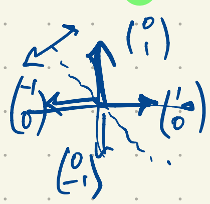
R^2:  $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

$R^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

H:  $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$$G = \text{symmetry group of square} \cong \Big\{ \underset{I}{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}, \underset{R}{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}, \underset{R^2}{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}}, \underset{R^3}{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}}, \underset{H}{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}, \underset{V}{\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}}, \underset{D}{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}, \underset{D'}{\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}} \Big\}$$

D:  $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

D': 

subgroup of $GL_2(\mathbb{R})$

$$\left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$$

$R^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ commutes with every element of G (not so immediately obvious from the other ways of representing G).

Similar to HW2 #4, 5 : $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ integers mod p.

e.g. $p = 3$, $F = \mathbb{F}_3 = \{0, 1, 2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\frac{1}{2} = 2$

$-\frac{1}{2} =$ $\quad -\frac{1}{2} = -2 = 1$