Lecture 5

Next Week
Quiz
- definitions (group, subgroup, center, abelian etc.)
- proofs that we've done in class/book
- problems/computation like homework problems

Next week the TA has office hours. Will be emailed about this.

The quiz will include today's material.

Permutations (subject of Chapter 5)
Last 2 weeks: focusing on cyclic groups (the simplest in some sense)

This week: focusing on permutation groups (the most complicated in some sense)
we'll only cover part of it.

Definition: Let A be a set. A permutation of A is a bijection $\varphi: A \to A$
i.e. a one-to-one and onto function.

Definition: A permutation group is a set of permutations of a set A that form a group under function composition.

Facts: If $\varphi: A \to A$ is a permutation
$\exists\ \varphi^{-1}: A \to A$ s.t. $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi =$ the identity function of A

We will focus on the case when A is a finite set. Moreover, we will usually take $A=\{1,2,3,4,5,\ldots,n\}$

Example: Let $A=\{1,2,3\}$
Let $\alpha: \{1,2,3\} \to \{1,2,3\}$
$\alpha(1)=2$
$\alpha(2)=1$
$\alpha(3)=3$

$\alpha \circ \alpha: \{1,2,3\} \to \{1,2,3\}$
$\alpha \circ \alpha(1) = 1$
$\alpha \circ \alpha(2) = 2$
$\alpha \circ \alpha(3) = 3$

The book: calls the identity function ε (in the context of permutation)
So $\varepsilon: \{1,2,3\} \to \{1,2,3\}$ is the identity permutation.
And we've seen $\alpha \circ \alpha = \varepsilon$

Now consider $H=\{\varepsilon,\alpha\}$. Is H a permutation group?

Yes it is

- H is closed under composition
- Are there inverse?
  $\alpha^{-1}=\alpha$ $(\alpha\circ\alpha=\varepsilon)$
  $\varepsilon^{-1}=\varepsilon$
- Associative? Yes, because function composition is always associatively.

Notation: We'll write $\alpha\beta$ for $\alpha\circ\beta$. And α^n for $\alpha\circ\alpha\cdots\circ\alpha$ if $n\geq 1$

$\alpha^0=\varepsilon$

$\alpha^{-n}=\alpha^{-1}\circ\cdots\circ\alpha^{-1}$

Notation for permutations

Sps: $\alpha:\{1,2,3,4\}\longrightarrow\{1,2,3,4\}$

s.t. $\alpha(1)=2$ $\alpha(2)=3$ $\alpha(3)=1$ $\alpha(4)=4$

* $\alpha=\begin{bmatrix}1&2&3&4\\2&3&1&4\end{bmatrix}$

Consider:

$\sigma=\begin{bmatrix}1&2&3&4&5\\2&4&3&5&1\end{bmatrix}$ $\gamma=\begin{bmatrix}1&2&3&4&5\\5&4&1&2&3\end{bmatrix}$

Then what is $\gamma\sigma=\begin{bmatrix}1&2&3&4&5\\4&2&1&3&5\end{bmatrix}$ $\sigma\gamma=\begin{bmatrix}1&2&3&4&5\\1&5&2&4&3\end{bmatrix}$

$\gamma\sigma\neq\sigma\gamma$ (compute RHS first)

Example: Let $S_3=\{\text{permutations of } \{1,2,3\}\}$

Let $\alpha\in S_3$. then there're 3 possibilities for $\alpha(1)$

Once $\alpha(1)$ is fixed $\longrightarrow$ 2 possibilities for $\alpha(2)\longrightarrow$ 1 possibility for $\alpha(3)$

So $3\times2\times1=6$ permutations.

$\varepsilon=\begin{bmatrix}1&2&3\\1&2&3\end{bmatrix}$ $\alpha_1=\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}$ $\alpha_3=\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}$ $\alpha_5=\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}$ $\alpha_4=\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}$ $\alpha_2=\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$

Claim: S_3 is a group Proof: clear

$|\varepsilon|=1$ $|\alpha_1|=2=|\alpha_2|=|\alpha_3|$ $|\alpha_4|=3=|\alpha_5|$

$\alpha_4^2=\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}=\alpha_5$ $\alpha_4^3=\begin{bmatrix}1&2&3\\1&2&3\end{bmatrix}=\varepsilon$

Example: S_n: (the symmetric group on n letters)

$S_n=\{\text{permutations of } \{1,2,3,\cdots,n\}\}$

Fact: S_n is a group.
Fact: $|S_n| = n!$

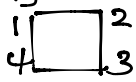
Proof: If α is a permutation. We have n choices for $\alpha(1)$, $(n-1)$ choices for $\alpha(2)$, $\cdots$ 1 choice for $\alpha(n)$.
So we have $n(n-1)(n-2)\cdots 1 = n!$ choices of α. ■

Prop: Let G be a finite group. Then if $x \in G$, $|x| \leq |G|$

Proof: Let $n = |x|$. Sps $n > |G|$
Let's look at $\langle x \rangle$. We proved that $|\langle x \rangle| = n$.
But $\langle x \rangle \leq G$. In particular, $\langle x \rangle \subseteq G$. So $|\langle x \rangle| \leq |G|$ ▨

note: $\langle x \rangle = \{e, x, x^2, \cdots, x^{n-1}\}$ n elements when $n = |x|$.

Example: Let's define a function (not a permutation) (example of a group nonomorphism)
$f: D_4 \to S_4$
For $x \in D_4$, $f(x)$ is the permutation of $\{1,2,3,4\}$ associated to x acting as a symmetgon

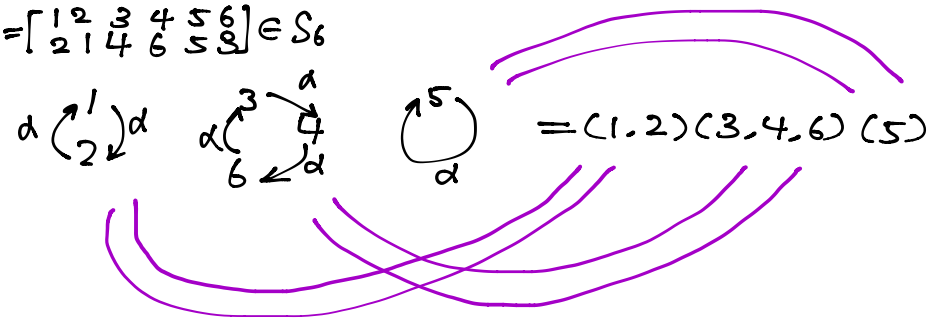


$f(R_0) = \varepsilon$
$f(R_{90}) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$ $\quad f(V) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$

$f(R_{180}) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}$ $\quad$ give an example of $\alpha \in S_4$ s.t. $\alpha \neq f(x)$ for any $x \in D_4$
$f(R_{270}) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$ $\quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$

Cycle notation:

$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix} \in S_6$



Def'n: Let $a_1, \cdots, a_m \in A$ be distinct elements ($a_i \neq a_j$ whenever $i \neq j$)
An expression $(a_1, a_2, \cdots, a_m)$ is called a cycle of length m or an m-cycle.
The expression $(a_1, \cdots, a_m)$ represents the following permutation α of A.
For $a_1, \cdots, a_m$:
$\alpha(a_i) = a_{i+1}$ (where $a_{m+1} = a_1$)
$\alpha(x) = x$ if $x \notin \{a_1, \cdots, a_m\}$

Example: $A = \{1,2,3,4,5,6\}$

Consider $(2,3,4,5)$ What permutation does it represent

$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 5 & 2 & 6 \end{bmatrix}$

What about $(1,2,3,1)$ This is not a valid cycle since 1 is repeated.

Let's work with $\{1,2,3,4,5,6\}$

$(5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} = \varepsilon$

$(3,4,6) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 5 & 3 \end{bmatrix}$

$(1,2) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{bmatrix}$

What is $(1,2)(3,4,6)(5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$

$(3,4,6)(1,2)(5) = [$ same thing $]$

Properties of Permutations

(1) Products of disjoint cycles

Thm: Every permutation of a finite set can be written as a product of disjoint cycles.

Proof: Let A be a finite set. (So keep in your mind $A = \{1, \cdots, n\}$)

Then consider α a permutation of A.

Let $a_1 \in A$

Consider $(a_1, \alpha(a_1), \alpha^2(a_1), \cdots, \alpha^{k-1}(a_1))$ where $\alpha^k(a_1) = a_1$

certainly $\alpha^n = \varepsilon$, in particular $\alpha^n(a_1) = a_1$

So pick k the smallest positive int. s.t $\alpha^k(a_1) = a_1$

This is a cycle of length k. i.e. we claim that $\{a_1, \alpha(a_1), \cdots, \alpha^{k-1}(a_1)\}$ are distinct. Sps $\alpha^i(a_1) = \alpha^j(a_1)$ where $i < j \leq k-1$

Then $\alpha^{j-i}(a_1) = a_1$

But $j - i < k$

Let $A_1 = \{a_1, \alpha(a_1), \cdots, \alpha^{k-1}(a_1)\}$

$A_2 = A \setminus A_1 = \{a \in A \mid a \notin A_1\}$

Then $\alpha(A_1) = A_1$, α restricted to A_1, is a permutation

Similarly, $\alpha(A_2) = A_2$. So α restricted to A_2, is a permutation.

So just repeat the process with A_2

By induction on $|A|$, we can assume α restricted to A_2 is a product of disjoint cycles $c_1, \cdots, c_k$.

Then α as a permutation of A is $(a_1, \alpha(a_1), \cdots, \alpha^{k-1}(a_1)), c_1, \cdots, c_n$.

Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 5 & 7 & 8 & 6 & 2 \end{bmatrix} = (1)(2,3,4,5,7,6,8)$

$A_1 = \{1\}$ $A_2 = \{2,3,4,5,6,7,8\}$

Q: Find $\alpha \in S_7$ that is a product of a 1-cycle, a 2-cycle and 4-cycle that are disjoint from one another.

Answer: $\alpha=(1)(2,3)(4,5,6,7)=(2,3)(1)(4,5,6,7)=(2,3)(1)(5,6,7,4)$
If we order the cycle decomposition by
- placing the smallest element 1st in each cycle.
- ordering the cycles by their 1st element.

The cycle decomposition is unique.
$(3,5,7)(8,2)(1,4,6)=(1,4,6)(2,8)(3,5,7)$

② Disjoint cycles commute
Thm: If $\alpha=(a_1,\cdots,a_k)$, $\beta=(b_1,\cdots,b_n)$
$a_i, b_j \in A$ and there distinct. i.e. $a_i \neq b_j \ \forall i,j$. Then $\alpha\beta=\beta\alpha$

Pf: $A_1=\{a_1,\cdots a_k\}$ $B_1=\{b_1,\cdots,b_n\}$, $C_1=A\setminus(A_1\cup B_1)=\{a\in A \mid a\in A_1 \text{ and } a\in B_1\}$
$A_1\cap B_1=\emptyset$
$A_1\cap C_1=\emptyset$
$B_1\cap C_1=\emptyset$

Moreover, $A=A_1\cup B_1\cup C_1$
If $a\in A_1$, Then $a=a_i$ for some i
What is $\alpha\beta(a)=\alpha(a)$ since $\beta(a)=a$
$\beta\alpha(a)=\alpha(a)$ since $\alpha(a)\in A$ So $\beta(\alpha(a))=\alpha(a)$
Similarly, if $b\in B_1$, what is $\alpha\beta(b)=\beta(b)$
$\beta\alpha(b)=\beta(b)$
Finally, if $c\in C_1$, $\alpha\beta(c)=c$, $\beta\alpha(c)=c$
Thus $\alpha\beta=\beta\alpha$ ∎

Prop: Let $\alpha=(a_1,\cdots,a_m)$ be a cycle of length m in S_n. Then $|\alpha|=m$

Proof: We want to show $\alpha^m=\varepsilon$, but $\alpha^k\neq\varepsilon$ for $1\leq k\leq m-1$.
If $x\notin\{a_1,\cdots,a_m\}$, $\alpha(x)=x$
If $a_i\in\{a_1,\cdots,a_m\}$, $\alpha(a_i)=a_{i+1}$ $(a_{m+1}<a_1)$

Similarly, $\alpha^j(a_i)=a_{i+j}$ (where $a_{m+1}=a_1$, $a_{m+2}=a_2$, ...)
So we see, $\alpha^j\neq\varepsilon$ for $1\leq j<m$ b/c $\alpha^j(a_1)=a_{1+j}\neq a_1$
But $\alpha^m(a_i)=a_{i+m}=a_i$
For $x\notin\{a_1,\cdots,a_m\}$, $\alpha^m(x)=x$, So we see $|\alpha|=m$. ∎

③ Order of a Permutation
Thm: Let $\alpha\in S_n$, $\alpha=c_1\cdots c_k$ be a decomposition of α into disjoint cycles
Then $|\alpha|=lcm(|c_1|,\cdots,|c_k|)$
$|c_j|=$ order $c_j=$ length of c_j

Proof: Let $\alpha=c_1\cdots c_k$. Sps $\alpha^l=\varepsilon$
Then $\alpha^l=(c_1\cdots c_k)^l$
$=\underbrace{c_1\cdots c_k c_1\cdots c_k\cdots c_1\cdots c_k}_{l \text{ times}}$
$=c_1\cdots c_1 c_2\cdots c_2\cdots c_k\cdots c_k=c_1^l c_2^l\cdots c_k^l=\varepsilon$

This implies $c_i^l = \varepsilon$
Sps $x \in \{1, \dots, n\}$. Then x appears in exactly one of the cycles c_i.
So $\alpha^l(x) = c_1^l \cdots c_n^l(x) = c_i^l(x)$

and $c_i^l(x) = \varepsilon(x)$ $\forall x \in \{1, \dots n\}$
iff: l is a multiple of $|c_i|$. Thus l is a multiple of each $|c_i|$. So the least possible l s.t. $\alpha^l = \varepsilon$ is $lcm(|c_1|, \dots, |c_k|)$

Example: Let $\alpha \in S_7$
What are the possibilities of $|\alpha|$? $7! = 720$
If we can find $l_1, \dots, l_k$ s.t. $l_i \geq 1$
$7 = l_1 + \cdots + l_k$ (this is called a partition of 7! We can consider α that can be written as $\alpha = c_1 \cdots c_k$ as a product of disjoint cycles where $|c_i| = l_i$
The order $|\alpha| = lcm(l_1, \dots, l_k)$

Def'n: If $\alpha \in S_n$. And $\alpha = c_1 \cdots c_k$ is a decomposition of α into disjoint cycles then the list $(|c_1|, |c_2|, |c_3|, \dots, |c_k|)$ is called the cycle-type of α.

What are the partitions of 7?

(7)
(6) (1)
(5) (2)
(5) (1) (1)
(4) (3)
(4) (2) (1)
(4) (1) (1) (1)
(3) (3) (1)
(3) (2) (2)
(3) (2) (1) (1)
(3) (1) (1) (1) (1) (1)
(2) (2) (2) (1)
(2) (2) (1) (1) (1)
(2) (1) (1) (1) (1) (1)
(1) (1) (1) (1) (1) (1) (1).

Transpositions + evenness/oddness of permutations
Def: Let (a_1, a_2) be a 2-cycle in S_n. We call all 2-cycles transpositions
Q: What's the order of any trans? Answer: 2

Lemma: If $\varepsilon = \beta_1 \cdots \beta_r$ is written as a product of transpositions. Then r must be even.

Pf: If $r = 1$, then $\varepsilon = (ij)$, which is a contradiction.
If $r = 2$, done.
Suppose $r > 2$. Write $\varepsilon = \beta_1 \cdots \beta_r$. Let $(ab) = \beta_r$
There're 4 possibilities for $\beta_{r-1}\beta_r$
Case ① $\beta_{r-1}\beta_r = (ab)(ab) = \varepsilon$ ✓
② $\beta_{r-1}\beta_r = (ac)(ab) = (ab)(bc)$
③ $\beta_{r-1}\beta_r = (bc)(ab) = (ac)(cb)$
④ $\beta_{r-1}\beta_r = (cd)(ab) = (ab)(cd)$

In ②③④, the last trans doesn't contain a.
Repeat this r times. If ① never occurs, the 1st trans will have a in it. But no later will one will. But this would imply $\varepsilon(a) \neq a$. $\rightarrow\leftarrow$. So ① must occur at some point.

review txtbk

Thm: If $\alpha \in S_n$, and $\alpha = \beta_1 \cdots \beta_r$ are decompositions of α into trans.
$\alpha = \gamma_1 \cdots \gamma_s$

$r \equiv s \bmod 2$

Pf: $\varepsilon = \alpha\alpha^{-1} = \beta_1 \cdots \beta_r \gamma_1^{-1} \cdots \gamma_s^{-1}$.

Note γ_i^{-1} is also a trans.
we have $\gamma_i^{-1} = \gamma_i$
So $r+s$ is even. Which is the same as $r \equiv s \bmod 2$.

Def'n: If $\alpha \in S_n$. Say α is even if when we write $\alpha = \beta_1 \cdots \beta_r$ as a product of the trans, r is even.
O.w., say α is odd.

Eg: Is $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$ even or odd?

$(132) = (1\ 2)(1\ 3)$

$(a_1, \cdots, a_m) = (a_1, a_m)(a_1, a_{m-1}) \cdots (a_1, a_3)(a_1, a_2)$

we see that $(a_1, \cdots a_m)$ is even if m is odd
odd if m is even.

Let $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$.

Prop: A_n is a subgroup of S_n.

Pf: Exercise.

Prop: If $n > 1$, $|A_n| = \frac{n!}{2}$

Pf: let $O_n = \{$the odd elements of $S_n\}$
Then we define $\varphi : A_n \to O_n$
by $\varphi(\alpha) = (1\ 2)\alpha$
Then φ is a bijection. b/c $\exists$ an inverse $\psi : O_n \to A_n$ given by
$\psi(\beta) = (1\ 2)\beta$

So $|O_n| = |A_n|$, But $S_n = A_n \cup O_n$ and $A_n \cap O_n = \emptyset$

So we see that $|A_n| = \frac{1}{2}|S_n|$