

§8 Groups of permutations

How do we model the idea of "transforming a system"?

Given a set A (collection of "things" in the system)

a permutation of the set A is given by a function $\phi: A \rightarrow A$ such that

- ϕ is one-to-one : $\phi(x) = \phi(y)$ only if $x = y$
(injective)
- ϕ is onto : any $a \in A$ is of the form $a = \phi(x)$
(surjective) for some x

Rem. this would model a reversible transform

the inverse map ϕ^{-1} is also a permutation of A

Consider the set of all permutations of A

(write S_A or $\text{Sym}(A)$)

Thm 8.5 S_A is a group with

- binary operation $\sigma \circ \tau$: composition of functions
 $\sigma \circ \tau(x) = \sigma(\tau(x))$
- identity elem. : $e = \text{id}_A$ the identity map on A
- inverse σ^{-1} : inverse map of σ

Proof we want the equalities

- $(\sigma \circ \tau) \circ \rho = \sigma \circ (\tau \circ \rho)$ associativity
- $e \circ \sigma = \sigma = \sigma \circ e$ for $e = \text{id}_A$
- $\sigma \circ \sigma^{-1} = e = \sigma^{-1} \circ \sigma$

as maps $A \rightarrow A$

Step 1 associativity : given input $a \in A$

$(\sigma \circ \tau) \circ \rho$ gives the output

$$(\sigma \circ \tau)(\rho(a)) = \sigma(\tau(\rho(a)))$$

$\sigma \circ (\tau \circ \rho)$ gives the same output

Step 2 $e \circ \sigma = \sigma$ etc. for $e = \text{id}_A$

$$e \circ \sigma(a) = e(\sigma(a)) = \text{id}_A(\sigma(a)) = \sigma(a)$$

Step 3 $\sigma \circ \sigma^{-1} = e$ etc.

$$\sigma \circ \sigma^{-1}(a) = \sigma(\sigma^{-1}(a)) = a = \text{id}_A(a) \quad \square$$

Rem S_n was a particular case of this

$$S_n = S_A \quad \text{for } A = \{1, 2, \dots, n\}$$

Isomorphism of permutation groups

Suppose we have two sets A, B and a function $f: A \rightarrow B$ that is both one-to-one and onto ("identification of two systems")

We can define an isomorphism of groups

$$\phi: S_A \rightarrow S_B \quad \text{by } \phi(\sigma) = f \circ \sigma \circ f^{-1}$$

(we get $\phi(\sigma \circ \tau) = \phi(\sigma) \circ \phi(\tau)$ from $f \circ \sigma \circ \overbrace{f^{-1} \circ f}^{\text{id}_A} \circ \tau \circ f^{-1} = f \circ \sigma \circ \tau \circ f^{-1}$)

$$\phi^{-1}: S_B \rightarrow S_A \quad \text{is given by } \phi^{-1}(\sigma') = f^{-1} \circ \sigma' \circ f$$

In particular when A has finitely many elems.

S_A is isomorphic to S_n for $n = |A|$

§9 Orbits, cycles

Fix A : set and $\sigma \in S_A$ (one-to-one & onto func. $A \rightarrow A$)

Given $a \in A$, the orbit of a under σ is

$$\{b \in A \mid b = \sigma^n(a) \text{ for some } n \in \mathbb{Z}\} \subset A$$

Observations

- if b is in the orbit of a , then orbit of b = orbit of a

$$\text{i.e. } b = \sigma^n(a) \Rightarrow c = \sigma^m(b) \text{ for some } m \\ \text{iff } c = \sigma^k(a) \text{ for some } k$$

$$\text{use } \sigma^m(b) = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a)$$

- we can partition A as a disjoint union of orbits : $A = \bigsqcup_{i \in I} (\text{orb. of } a_i) \quad \text{for some } (a_i)_{i \in I}$

Ex. $A = \{1, 2, 3, 4\}$ $\sigma(1) = 4, \sigma(2) = 1, \sigma(3) = 3, \sigma(4) = 2$
 orb. of 1 = $\{1, 4, 2\}$ = orb. of 2 = orb. of 4
 orb. of 3 = $\{3\}$

Def. a cycle is a permutation $\sigma \in S_A$ such that
 there is at most one nontrivial orbit ~~for~~ σ under
 (the other orbits should be of the form $\{b\}$)
 i.e. (assuming $|A| < \infty$) $\exists$ seq. $a_1, \dots, a_k$ in A
 s.t. $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$
 $\sigma(b) = b$ for other elements b

Ex. the above example for $A = \{1, \dots, 4\}$
 $\sigma = (1\ 4\ 2)$

Notation $(a_1\ a_2\ \dots\ a_k)$ for this σ ; cycle of length k

Thm 9.8 Suppose $|A| < \infty$

Given $\sigma \in S_A$, we can find disjoint subsets

$B_1, \dots, B_r$ in A s.t. $\sigma = (b_1^{(1)} \dots b_{k_1}^{(1)}) (b_1^{(2)} \dots b_{k_2}^{(2)}) \dots (b_1^{(r)} \dots b_{k_r}^{(r)})$
 with $B_i = \{b_1^{(i)}, \dots, b_{k_i}^{(i)}\}$

Proof (sketch) take the orbits under σ as B_i 's

choose some $b_1^{(i)} \in B_i$, then take $b_2^{(i)} = \sigma(b_1^{(i)})$

$\dots$ continue until we see

$$\sigma(b_k^{(i)}) = b_1^{(i)} \quad \square$$

Obs. $(a_1\ a_2\ \dots\ a_k) = (a_1\ a_k) \dots (a_1\ a_3) (a_1\ a_2)$

$\Rightarrow$ any $\sigma \in S_A$ is a product of cycles of length 2
 (transpositions)

Rem there can be different ways to write σ as
 a prod. of transpositions

$$\text{ex. } (1, 3) (2, 3) (1, 3) = (1, 2)$$

Thm 9.15 Suppose $|A| < \infty$, and fix $\sigma \in S_A$

The parity of k for $\sigma = \tau_1 \dots \tau_k$ (τ_i : transp.) is well-defined

Proof. (sketch) Assuming $A = \{1, \dots, n\}$ Define the inversion number

$$\text{Inv}(\sigma') = \text{number of } (i, j) \text{ s.t. } i < j \text{ and } \sigma'(i) > \sigma'(j) \quad (1) \\ 1 \leq i, j \leq n$$

Then check $\text{Inv}(\tau \sigma') = \text{Inv}(\sigma') \pm 1$ for transp. τ

This gives $\text{Inv}(\sigma) \equiv k \pmod{2}$ if $\sigma = \tau_1 \dots \tau_k$
 τ_i transp. $\square$

Similar rel. holds for $|\text{Orb}(\sigma)| = \text{num. of orbits of } \sigma$

We say σ is an even permutation if $\sigma = \tau_1 \dots \tau_{2k}$
and odd perm. if $\sigma = \tau_1 \dots \tau_{2k+1}$ for some k