GROUP THEORY

5TH SEMESTER - LECTURE 4
BY

NILOFAR NAHID

DEPARTMENT OF MATHEMATICS
MAHARAJA MANINDRA CHANDRA COLLEGE

August 24, 2020

Group action

Theorem

Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1, a_2, \ldots, a_{k_1})(b_1, b_2, \ldots, b_{k_2}) \ldots.$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1), \tau(a_2), \ldots, \tau(a_{k_1}))(\tau(b_1), \tau(b_2), \ldots, \tau(b_{k_2})) \ldots$$

i.e., $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$ (including its 1 -cycles) then the integers $n_1, n_2, \ldots, n_r$ are called the cycle type of σ.

The cycle type of a permutation is unique. For example, the cycle type of an m-cycle in S_n is $1, 1, \ldots, m$, where the m is preceded by $n - m$ ones.

The cycle type of an 2-cycle in S_3 is $1, 2$ and cycle type of an 3-cycle is 3.

Theorem

Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.

Proof. By above theorem, conjugate permutations have the same cycle type. Conversely, let $\sigma, \rho \in S_n$ both be of cycle type $(k_1, k_2, \ldots, k_l)$ and we show that σ and ρ are conjugate in S_n. Let σ and τ be written as products of disjoint cycles as

$$\sigma = \alpha_1\alpha_2\ldots\alpha_l \text{ and } \rho = \beta_1\beta_2\ldots\beta_l,$$

where α_i and β_i are k_i-cycles. For each i let us write

$$\alpha_i = (a_{i1}a_{i2}\ldots a_{ik_i}) \text{ and } \beta_i = (b_{i1}b_{i2}\ldots b_{ik_i}).$$

Now define τ by $\tau(a_{ij}) = b_{ij}$ for every i, j such that

$$1 \le i \le l \text{ and } 1 \le j \le k_i.$$

Hence we have $\tau\alpha_i\tau^{-1} = \beta_i$. So, we have

$$\tau\sigma\tau^{-1} = (\tau\alpha_1\tau^{-1})(\tau\alpha_2\tau^{-1})\ldots(\tau\alpha_l\tau^{-1}) = \beta_1\beta_2\ldots\beta_l = \rho.$$

So, any two elements of S_n with the same cycle type are in the same conjugacy class.

Proof. Each distinct cycle type in S_n represents a distinct partition of n, and each cycle type represents a conjugacy class. Since there is a bijection between the conjugacy classes of S_n and the permissible cycle types (because conjugates are the same cycle type). The result follows. The second assertion of the theorem follows, completing the proof.

If n = 3, the partitions of 3 and corresponding representatives of the conjugacy classes of S_3 (with 1 -cycles not written) are as given in the following table:

partition of 3	Representative of Conjugacy Class
$1+1+1$	e
$1+2$	(12)
3	(123)

If n = 4, the partitions of 4 and corresponding representatives of the conjugacy classes of S_4 (with 1 -cycles not written) are as given in the following table:

partition of 4	Representative of Conjugacy Class
$1+1+1+1$	e
$1+1+2$	(12)
$2+2$	$(12)(34)$
$1+3$	(123)
4	(1234)

Group action

If n = 5, the partitions of 5 and corresponding representatives of the conjugacy classes of S_5 (with 1 -cycles not written) are as given in the following table:

partition of 5	Representative of Conjugacy Class
$1+1+1+1+1$	e
$1+1+1+2$	(12)
$1+1+3$	(123)
$1+4$	(1234)
5	(12345)
$1+2+2$	$(12)(34)$
$2+2$	$(12)(34)$
$2+3$	$(12)(345)$

A finite group is called **simple** when it is nontrivial and its only normal subgroups are the trivial subgroup and the whole group.

For instance, a finite group of prime order is simple, since it in fact has no non-trivial proper subgroups at all (normal or not). A finite abelian group G not of prime order, is not simple: let p be a prime factor of $|G|$, so G contains a subgroup of order p, which is a normal since G is abelian and is proper since $|G| > p$. Thus, the abelian finite simple groups are the groups of prime order.

Lemma 1

For $n \geq 3$, A_n is generated by 3-cycles. For $n \geq 5$, A_n is generated by permutations of type $(2, 2)$.

Lemma 2

For $n \geq 5$, any two 3-cycles in A_n are conjugate in A_n.

Lemma 3

When $n \geq 5$ and $\sigma \neq e$ in A_n has conjugate $\sigma' \neq \sigma$ such that $\sigma(i) = \sigma'(i)$ for some i.

Note that two elements of the same cycle type need not be conjugate in A_5.

Theorem

The group A_5 is simple.

Proof. We want to show the only normal subgroups of A_5 are $\{e\}$ and A_5. Let N be the normal subgroup of A_5 with $|N| > 1$. We will show N contains a 3-cycle. It follows that $N = A_5$ by Lemmas 1 and 2. Pick $\sigma \in N$ with $\sigma \neq e$. The cycle structure of σ is $(abc), (ab)(cd) or (abcde)$ where different letters represent different numbers. Since we want to show N contains a 3-cycle, we may suppose σ has the second or third cycle type. In the second case, N contains

$$((abe)(ab)(cd)(abe)^{-1})(ab)(cd) = (be)(cd)(ab)(cd) = (aeb).$$

In the third case, N contains

$$((abc)(abcde)(abc)^{-1})(abcde)^{-1} = (adebc)(aedcb) = (abd).$$

Therefore N contains a 3-cycle, so $N = A_5$.

Theorem

For $n \geq 5$, A_n is simple.

Proof. We may suppose $n \geq 6$. For $1 \leq i \leq n$, let A_n act in the natural way on $\{1, 2, \ldots, n\}$ and let $H_i \subset A_n$ be the subgroup fixing i, so $H_i \cong A_{n-1}$. By induction, each H_i is simple. Note each H_i contains a 3-cycle. Let N be the nontrivial normal subgroup of A_n. We want to show $N = A_n$. Pick $\sigma \in N$ with $\sigma \neq e$. By lemma 3 there is a conjugate σ' of σ such that $\sigma' \neq \sigma$ and $\sigma(i) = \sigma'(i)$ for some i. Since N is normal in A_n , $\sigma' \in N$. Then $\sigma^{-1}\sigma'$ is a non-identity element of N which fixes i, so $N \bigcap H_i$ is a non-trivial subgroup of H_i. It is also a normal subgroup of H_i since N is normal in A_n. Since H_i is simple,

$$N \bigcap H_i = H_i.$$

Therefore $H_i \subset N$. Since H_i contains a 3-cycle, N contains a 3-cycle and we are done.

Group action

One can analogously define the notion of a right group action of the group G on the nonempty set A as a map from $A \times G \to A$, denoted by $a \cdot g$ for $a \in A$ and $g \in G$ that satisfies the axioms:

1. $(a \cdot g_1) \cdot g_2 = a \cdot (g_1 g_2)\ \forall\ a \in A$, and $g_1, g_2 \in G$
2. $a \cdot e = a,\ \forall a \in A.$

If G acts on itself by conjugation, then conjugation is written as a right group action using the following notation:

$$a^g = g^{-1} a g, \ \ \forall \ \ a, g \in G.$$

For arbitrary group actions it is an easy exercise to check that if we are given a left group action of G on A then the map $A \times G \to A$ defined by $a \cdot g = g^{-1} \cdot a$ is a right group action. Conversely, given a right group action of G on A we can form a left group action by $g \cdot a = a \cdot g^{-1}$. Call these pairs corresponding group actions. Put another way, for corresponding group actions, g acts on the left in the same way that g^{-1} acts on the right. This is particularly transparent for the action of conjugation because the "left conjugate of a by g," namely gag^{-1} is the same group element as the "right conjugate of a by g^{-1} namely by $a^{g^{-1}}$. Thus two elements or subsets of a group are "left conjugate" if and only if they are "right conjugate," and so the relation "conjugacy" is the same for the left and right corresponding actions.

Sylow's theorem

Definition.

Let G be a group and let p be a prime.

1. A group of order p^{α} for some $\alpha \geq 1$ is called a p-group. Subgroups of G which are p-groups are called p-subgroups.

2. If G is a group of order $p^{\alpha}m$, where p does not divide m, then a subgroup of order p^{α} is called a Sylow p-subgroup of G.

3. The set of Sylow p-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$.

Theorem

If $H, K$are subgroups of G and H is a subgroup of $N_G(K)$, then HK is a subgroup of G.

Proof. We prove $HK = KH$. Let $h \in H, k \in K$. By assumption, $hkh^{-1} \in K$, hence

$$hk = (hkh^{-1})h \ \in KH.$$

This proves that $HK \subseteq KH$. Similarly

$$kh = h(h^{-1}kh) \ \in HK$$

proving the reverse containment.

Lemma

Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.

Proof. Let $H = N_G(P) \cap Q$. Since P is a subgroup of $N_G(P)$ it is clear that $P \cap Q \leq H$, so we must prove the reverse inclusion. Since by definition $H \leq Q$ this is equivalent to showing $H \leq P$. We do this by demonstrating that PH is a p-subgroup of G containing both P and H; but P is a p-subgroup of G of largest possible order, so we must have $PH = P$, i.e., $H \leq P$.

Since $H \leq N_G(P)$, hence by above theorem PH is a subgroup. Also

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

All the numbers in the above quotient are powers of p, so PH is a p-group. Moreover, P is a subgroup of PH so the order of PH is divisible by p^α, the largest power of p which divides $|G|$. These two facts force $|PH| = p^\alpha = |P|$. This in turn implies $P = PH$ and $H \leq P$. This establishes the lemma.