Algebra MATH-310

Lecture 6

Anna Lachowska

October 28, 2024

Plan of the course

1. Integers: 1 lecture
2. Groups: 6 lectures
3. Rings and fields: 5 lectures
4. Review: 1 lecture

Today: Groups: lecture 5

(a) Transpositions in S_n

(b) Sign of a permutation in S_n

(c) The alternating group A_n

(d) Conjugacy classes in S_n

(e) Action of a group on a set by permutations

(f) The orbit-stabilizer theorem and the class equation of a finite group

Recall: Symmetric group S_n

- A cycle $(i_1, i_2, \dots i_n)$ is a permutation that sends $i_1 \to i_2$, $i_2 \to i_3$, ... $i_k \to i_1$ and stabilizes the remaining elements.
- Two cycles $(i_1, i_2, \dots i_k) \in S_n$ and $(j_1, j_2, \dots j_m) \in S_n$ are disjoint if and only if $i_t \neq j_p$ for all t and p.
- Disjoint cycles commute in S_n: if $i_t \neq j_p$ for all t and p, then $(i_1, i_2, \dots i_k)(j_1, j_2, \dots j_m) = (j_1, j_2, \dots j_m)(i_1, i_2, \dots i_k)$.
- Any $\sigma \in S_n$ can be written as a product of disjoint cycles $\sigma = (\ )(\quad)(\quad)\dots(\ )$ uniquely up to the order of the cycles.
- In S_n we have $\pi(i_1, i_2, \dots i_k)\pi^{-1} = (\pi(i_1), \pi(i_2), \dots \pi(i_k))$.
- A transposition is a 2-cycle in S_n.

Every k-cycle is a product of $(k-1)$ transpositions.

$(123) = (13)(12)$

Corollary

The group S_n is generated by transpositions $\{(ij)\}_{1 \le i < j \le n}$.

Proof: Any $\sigma \in S_n$ is a product of disjoint cycles

Every cycle is a product of transpositions

$\Rightarrow$ Every $\sigma \in S_n$ can be written as a product of transpositions ▨

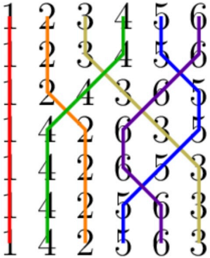
Remark: This presentation is not unique.

$$(13) = \underbrace{(12)}_{\pi}\underset{\rho}{(23)}\underbrace{(12)}_{\pi^{-1}}$$

$(12)(46) = (46)(12)$

Any element of S_n is a product of transpositions

A transposition (ij) can be visualized as a crossing of two lines that correspond to elements i and j. Then any element $\sigma \in S_n$ can be represented as a tangle of threads. Each intersection corresponds to a transposition.



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

$$\longleftarrow$$

$$\sigma = (56)(35)(24)(36)(34)(56) = (1)(24563) = (24563)$$

The sign of a permutation: ± 1, $\overset{+1}{\text{even}}$ or $\overset{-1}{\text{odd}}$

Definition

An inversion in the ordered set $\{a_1, a_2, \dots a_n\}$ is a couple $a_i > a_j$, where $i < j$.

No inversion: 123456

1 inversion: $12\underset{\leftrightarrows}{43}56$

461235 $\quad$ $3 + 4 = 7$ inversions

Theorem

Let $\sigma \in S_n$ be given as a product of transpositions. Then the number of transpositions in σ has the same parity as the number of inversions in $\sigma(1, 2, \dots n)$.

Idea:

$$\sigma(1\,2 \dots n) = a_1 a_2 \dots i\, b_1 b_2 \dots j\, c_1 c_2 \dots$$

Action of (ij), how does it change # of inversions in the string above?

$$a_1 a_2 \dots j\, b_1 b_2 \dots i\, c_1 c_2 \dots = (ij)\sigma(1 2 \dots n)$$

a_k, c_k do not contribute to the change of # of inversions

If $b_k > i$ and $b_k > j$ or $b_k < i$ and $b_k < j$ $\Rightarrow$ also does not change

If $i < b_k < j$ or $j < b_k < i$: $i \underset{<}{\cdots} b_k \underset{<}{\cdots} j \Rightarrow \underbrace{j \cdots b_k}_{\text{inversion}} \underbrace{\cdots i}_{\text{inversion}}$

In this case for each b_k the # of inversions changes by ± 2

Finally, $i \leftrightarrow j$ adds or subtracts 1 inversion.

$\Rightarrow$ Totally, action by a transposition changes # of inversions by an odd number.

$\sigma = 1 \Rightarrow \sigma(12..n) = 12....n$ no inversions

$\sigma = (ij) \Rightarrow$ odd # of inversions in $\sigma(1,2...n)$

$\sigma = (k\ell)(ij) \Rightarrow$ odd + odd = even # of inversions in $\sigma(12..n)$

etc.

▨

Theorem

A product of an odd number of transpositions cannot be equal to a product of an even number of transpositions in S_n.

parity of the number of transpositions in σ equals to the parity of # of inversions in $\sigma(1....n)$

The sign of a permutation

Definition

Let $\sigma \in S_n$. Then $\mathrm{sgn}(\sigma) = (-1)^{|\text{transpositions in } \sigma|}$.

$\mathrm{sgn}(\sigma) = 1 \iff \sigma =$ even # of transpositions

$\mathrm{sgn}(\sigma) = -1 \iff \sigma =$ odd # of transpositions

Proposition

$\mathrm{sgn} : S_n \to \{\pm 1\}$ *is a group homomorphism.*

Proof:

$$\mathrm{sgn}(\sigma \cdot \tau) = (-1)^{\#\text{transp}(\sigma\cdot\tau)} = (-1)^{\#\text{transp}(\sigma) + \#\text{transp}(\tau)} =$$

$$= (-1)^{\#\text{transp}(\sigma)} \cdot (-1)^{\#\text{transp}(\tau)} = \mathrm{sgn}(\sigma)\cdot \mathrm{sgn}(\tau)$$

$$\mathrm{sgn}(1) = 1^0 = 1$$

Recall: The kernel of a group homomorphism is a normal subgroup.

$\ker(\mathrm{sgn}) \lhd S_n$ normal subgroup

The alternating group A_n

$\varphi : G \to H$

$\ker\varphi \trianglelefteq G \qquad G/\ker\varphi \underset{\sim}{\to} H$

Definition

The alternating group A_n is $A_n = \ker(\mathrm{sgn}) \trianglelefteq S_n$. It consists of all even permutations in S_n.

By Lagrange's theorem, $|S_n| = |A_n| \cdot |\{\pm 1\}| = 2|A_n|$.

k-cycle = product of (k-1) transpositions

$(123) = (13)(12)$

Example: $S_3 = \{\underset{\text{even}}{1}, \underset{\text{odd}}{(12)}, \underset{\text{odd}}{(13)}, \underset{\text{odd}}{(23)}, \underset{\text{even}}{(123)}, \underset{\text{even}}{(132)}\}$.

$A_3 = \{1, (123), (132)\} \qquad |A_3| = 3 = \frac{6}{2}$

$$|A_n| = \frac{|S_n|}{2}$$

Recall: the cycle type of $\sigma \in S_n$ is preserved by conjugation

Moreover, any element of type $(i_1, i_2, \dots i_k)$ can be obtained from any other element of the same type by conjugation.

Definition

The conjugacy class of an element h in a group G is the set of elements $\{ghg^{-1}\}_{g\in G}$.

Corollary

S_n is a disjoint union of conjugacy classes. Each conjugacy class is determined by the set of lengths of disjoint cycles. The conjugacy classes in S_n are in bijection with the partitions of the number n:

$$n = i_1 + i_2 + \dots i_k; \qquad i_1 \geq i_2 \geq \dots \geq i_k \geq 1,$$

where $\{i_1, i_2, \dots i_k\}$ are the lengths of the cycles in the disjoint cycle decomposition of elements in the given conjugacy class.

Conjugacy classes in S_n

Example: $G = S_4$.

Conjugacy classes ↔ partitions of 4. : $\{4\}, \{3,1\}, \{2,2\}, \{2,1,1\}, \{1,1,1,1\}$

$\{4\}$ 4-cycles $(1234), (3142) \ldots$ $\frac{4!}{4} = 3! = 6$

$\{3,1\}$ 3-cycles $(123), (423), \ldots$ $\binom{4}{3} \cdot 2 = 8$

$\{2,2\}$ products of 2 disjoint 2-cycles $(12)(34)$ $\binom{4}{2} \cdot \frac{1}{2} = 3$

$\{2,1,1\}$ 2-cycles $(12), (13)$ $\binom{4}{2} = 6$

$\{1,1,1,1\}$ the trivial elt 1 1

$6+8+3+6+1 = 24$

$|S_4| = 4! = 24$

Conclusions: the group S_n

- Any element $\sigma \in S_n$ is a product of an odd or an even number of transpositions. The sign of σ is determined by the parity of the number of transpositions in σ.
- The alternating group A_n is the kernel of the group homomorphism $\phi : S_n \to \{\pm 1\}$ given by $\sigma \to sgn(\sigma)$. It consists of all even permutations in S_n.
- The conjugacy class of $\sigma \in S_n$ is completely determined by the cycle type of σ.
- The conjugacy classes in S_n are in bijection with the partitions of number n.

Action of a group on a set

Definition

A finite group G acts on a finite set E if for any $g \in G$, any $x \in E$ the element $g(x) \in E$ is defined, and $1(x) = x$ and $g_1 g_2(x) = g_1(g_2(x))$ for any $g_1, g_2 \in G$ and any $x \in E$.

Example: S_n acting on $E = \{1, 2, \ldots n\}$

Definition

The set $Orb_x = \{g(x)\}_{g \in G}$ is the orbit of the element $x \in E$ under the action of the group G.

We have

$g_1 x = g_2 y \Rightarrow y = g_2^{-1} g_1 x \in Orb_x$

Similarly $x \in Orb_y$

$\Rightarrow Orb_x = Orb_y$

1. $Orb_x = Orb_y$ or $Orb_x \cap Orb_y = \emptyset$. (Exercise)
2. Every element of E belongs to an orbit.
3. Therefore, $E = \cup_{i=1}^{r} Orb_{x_i}$, where $\{x_i\}_{i=1}^{r}$ is a complete set of representatives of the orbits.

Action of a group on itself by conjugations

Action of a finite group on itself by conjugation is an example of a group acting on a set by permutations:

$$g : G \to G \qquad g : h \to ghg^{-1}.$$

$1(h) = 1h1 = h$; $(g_1 g_2)(h) = (g_1 g_2) h (g_1 g_2)^{-1} = g_1 (g_2 h g_2^{-1}) g_1^{-1} =$

$\forall h \in G$ $\quad = g_1(g_2(h)).$ $\quad \forall h \in G, g_1, g_2 \in G.$

Then $Orb_h = \{ghg^{-1}\}_{g \in G} \equiv C_h$ is the conjugacy class of h in G.

Therefore, any finite group is a disjoint union of its conjugacy classes:

$$G = \cup_{i=1}^{r} C_{h_i}.$$

Conjugacy classes in G

Remark

If G is abelian, then $C_h = \{ghg^{-1}\}_{g\in G} = \{gg^{-1}h\}_{g\in G} = \{h\}$. Therefore, each conjugacy class contains exactly one element and the number of conjugacy classes equals to $|G|$.

The stabilizer subgroup

Definition

Let G act on a set E by permutations. If $x \in E$, then

$$Stab_x = \{g \in G : g(x) = x\}$$

is the stabilizer subgroup of x in G.

Proposition

The stabilizer $Stab_x \subset G$ is a subgroup in G.

Proof:

(1) $1(x) = x \quad \forall x \Rightarrow 1 \in Stab_x$

(2) If $g_1, g_2 \in Stab_x \Rightarrow g_1 \underbrace{g_2(x)}_{=x} = \underbrace{g_1(x)}_{=x} = x \Rightarrow g_1 g_2 \in Stab_x$

$g \cdot x = x \Rightarrow (g^{-1}g)x = x$

$= g^{-1}(gx) = g^{-1}(x) = x \Rightarrow g^{-1} \in Stab_x$ ▨

The orbit-stabilizer theorem

Theorem

Let a finite group G act on a finite set E, and $x \in E$. Then

$$|Orb_x| = [G : Stab_x] = |G|/|Stab_x|.$$

Proof: Let $H = Stab_x \subset G$ and consider the left cosets wrt H in G

Then: $\mu : \{gH\}_{g \in G} \longrightarrow Orb_x$ is a bijection

$\mu : gH \longrightarrow g \cdot x \quad \forall g \in G$. μ is surjective: $\forall g \in G$ belongs to a coset.

Suppose $\mu(g \cdot H) = \mu(f \cdot H) \in Orb_x \Rightarrow g \cdot x = f \cdot x \Rightarrow f^{-1} g \cdot x = x$

$\Rightarrow f^{-1} g \in H = Stab_x \Rightarrow f^{-1} g H \subset H \Rightarrow gH \subset fH$

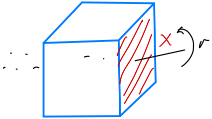
Similarly $fH \subset gH$ $\quad \Rightarrow gH = fH$

$\Rightarrow \mu$ is injective $\Rightarrow \mu$ is bijective $\Rightarrow$ # H-cosets $= \frac{|G|}{|H|} = |Orb_x|$

$\Rightarrow |Orb_x| = \frac{|G|}{|Stab_x|}$ ▨

Application: the order of the rotational symmetries of a cube

Let G be the group of rotational symmetries of a cube. Then G acts on the set of faces E of the cube by permutations.



$$|Orb_x| = \frac{|G|}{|Stab_x|}$$

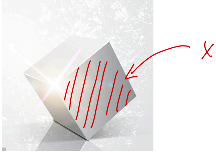
$Stab_x = \{1, r, r^2, r^3\}$ where r is a rotation by $\frac{\pi}{2}$

$$|Stab_x| = 4$$

$$|Orb_x| = 6$$

$$\Rightarrow \quad |G| = |Orb_x| \cdot |Stab_x| = 24$$

Poll: All isometries of a cube



Let K be the group of all isometries of a cube: compositions of rotations and reflections in $\mathbb{R}^3$ that preserve the cube. Then the order of K is

A: 24

[✓ B: 48]

C: 56

D: 72

E: 60

Action of K on the set of faces;

$|Orb_x| = 6$; $Stab_x = D_4 \Rightarrow |Stab_x| = 8$

dihedral gp of symmetries of a square

$\Rightarrow |G| = |Orb_x| \cdot |Stab_x|$

$|G| = 6 \cdot 8 = 48.$

Centralizer of an element of G

Definition

The center of a group $Z(G) \subset G$ is the set of all elements that commute with any $g \in G$.

$$Z(G) = \{x \in G : xg = gx \ \forall g \in G\}$$
$$= \{x \in G : gxg^{-1} = x \ \forall g \in G\}$$
$$= \text{all 1-elt conjugacy classes in } G$$

Definition

The centralizer of an element $x \in G$ is the subgroup $G_x = \{g \in G : gxg^{-1} = x\}$. In other words, the centralizer of $x \in G$ the stabilizer of $x \in G$ with respect to the action of G on itself by conjugation.

The class equation of a finite group

Theorem

The class equation of G *is*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |C_{x_i}| = |Z(G)| + \sum_{i=1}^{r} [G : G_{x_i}],$$

where C_{x_i} *are all the nontrivial (with more than one element) conjugacy classes, and* G_{x_i} *are the centralizer subgroups:*
$G_{x_i} = \{g \in G : g x_i g^{-1} = x_i\}$.

$$|G| = \underbrace{\sum_{i=1}^{m} |C_{x_i}|}_{\text{disjoint union of conj classes}} = \underbrace{\sum_{i=1}^{t} |C_{x_i}|}_{\text{1-elt conj classes}} + \sum_{j=1}^{r} |C_{x_j}|$$

nontrivial conj classes

$$|G| = \overset{\|}{|Z(G)|} + \sum_{j=1}^{r} |C_{x_j}| = |Z(G)| + \sum_{j=1}^{r} \frac{|G|}{|G_{x_j}|}$$

$|C_{x_j}| = [G : G_{x_j}]$ // by the orbit-stabilizer theorem ▨

Application: groups of prime power order

Proposition

A group of order p^n, where p is a prime, has a nontrivial center.

Proof: Class equation of G

$$p^n = \underbrace{|G|}_{\text{divisible by } p} = |Z(G)| + \sum_{j=1}^{r} \underbrace{[G:G_{x_j}]}_{>1}$$

$\downarrow$ divisible by p

$G_{x_j} \subset G \Rightarrow |G_{x_j}|$ divides $|G| = p^n$

$\Downarrow$

$|Z(G)|$ is also divisible by p. ; $|Z(G)| \geq 1$ contains the trivial elt

$\Rightarrow$ $|Z(G)|$ is a nontrivial multiple of p

$\geq p$ elements in $Z(G)$.

▨