Algebra MATH-310

Lecture 6

Anna Lachowska

October 27, 2025

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) Sign of a permutation in S_n
(b) The alternating group A_n
(c) Conjugacy classes in S_n

S_n

groups in general

(d) Action of a group on a set by permutations
(e) The orbit-stabilizer theorem and the class equation of a finite group
(f) Cauchy's theorem: If a group's order is divisible by a prime p, then it contains an element of order p

Recall: Symmetric group S_n

- A cycle $(i_1, i_2, \ldots i_n)$ 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 $(i_1, i_2, \ldots i_k) \in S_n$ and $(j_1, j_2, \ldots j_m) \in S_n$ 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 $(i_1, i_2, \ldots i_k)(j_1, j_2, \ldots j_m) = (j_1, j_2, \ldots j_m)(i_1, i_2, \ldots i_k)$.
- Any $\sigma \in S_n$ can be written as a product of disjoint cycles $\sigma = (\ )(\ \ )(\ \ )\ldots(\ )$ uniquely up to the order of the cycles.
- In S_n we have $\pi(i_1, i_2, \ldots i_k)\pi^{-1} = (\pi(i_1), \pi(i_2), \ldots \pi(i_k))$.
- A transposition is a 2-cycle in S_n. An inversion in a string of numbers is the situation when a bigger number goes before a smaller number.
- If σ is a permutation of the string $(1, 2, \ldots n)$, then the number of transposition in any expression of σ has the same parity as the number of inversions in the resulting string $\sigma(1, 2, \ldots n)$.

The sign of a permutation

Ex: $(12)(12) = 1$

2 transp. 0 transp.

Theorem

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

The parity of # of transpositions in σ is equal to the parity of # of inversions in $\sigma(1\ 2\ 3\ \ldots n)$

The sign of a permutation

Definition

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

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

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

Proposition

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

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

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

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

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

$\ker(\operatorname{sgn}) \trianglelefteq S_n$ normal subgroup.

The alternating group A_n

Definition

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

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

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

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

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

even odd odd odd even even

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

$A_3 \simeq C_3 = \langle t : t^3 = 1 \rangle$

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

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

Moreover, any element of type $(i_1, i_2, \ldots i_k)$ 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:

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

where $\{i_1, i_2, \ldots i_k\}$ 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 $\leftrightarrow$ partitions of 4. $\{4\}, \{3,1\}, \{2,2\}, \{2,1,1\}, \{1,1,1,1\}$

$\{4\}$ 4-cycles $(1234), (1243), \ldots$ $\quad \frac{4!}{4} = 3! = 6$

$\{3,1\}$ 3-cycles $(132), (324)$ $\quad \binom{4}{3} \cdot 2 = 8$

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

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

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

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

$|S_4| = 4! = 24$.

☺

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 $Orb_x \cap Orb_y \neq \emptyset \Rightarrow g_1 x = g_2 y \Rightarrow y = g_2^{-1} g_1 x \in Orb_x$

Similarly $x \in Orb_y \Rightarrow Orb_x = Orb_y$

1. $Orb_x = Orb_y$ or $Orb_x \cap Orb_y = \emptyset$. ✓
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:

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

$(g_1 g_2)(h) = (g_1 g_2) h (g_1 g_2)^{-1} = g_1 (g_2 h g_2^{-1}) g_1^{-1} = g_1 (g_2 (h))$ $\forall h \in G$ $\forall g_1, g_2 \in G$

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 of x in G.

Proposition

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

Proof: (1) $1(x) = x$ $\forall x \in E \Rightarrow 1 \in Stab_x$

(2) If $g_1, g_2 \in Stab_x \Rightarrow g_1 g_2 (x) = g_1 (g_2(x)) = g_1(x) \Rightarrow g_1 g_2 \in Stab_x$

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

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

The orbit-stabilizer theorem

$Orb_x = \{g \cdot x\}_{g \in G}$

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

$\mu: gH \xrightarrow{def} g \cdot x$ $\forall g \in G \Rightarrow \mu$ is surjective: $\forall g \in G$ belongs to a left H-coset

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

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

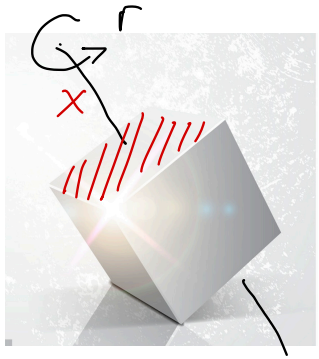
Similarly $fH \subset gH$

$\Rightarrow \mu$ is injective $\Rightarrow \mu$ is bijective $\Rightarrow$ # of 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.



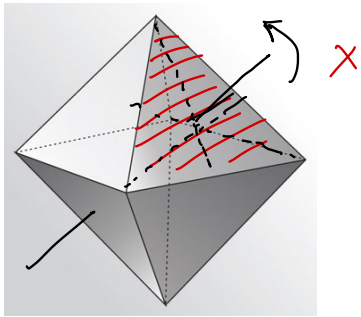
$$|Orb_x| = \frac{|G|}{|Stab_x|}$$

$Stab_x = \{1, r, r^2, r^3\}$ rotations of this face by $\frac{\pi}{2}, \pi, \frac{3\pi}{2}$

$|Stab_x| = 4$

$|Orb_x| = 6$ $\Rightarrow$ $|G| = |Stab_x| \cdot |Orb_x| = 24.$

Poll: All isometries of an octahedron



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

A: 60

B: 16

C: 48

D: 24

E: 32

K acts by permutation on faces

$|Orb_x| = 8$

$6 = |Stab_x| = \{$rotations by $\frac{2\pi}{3}, \frac{4\pi}{3}$, 3 reflections$\}$ (1)

$\cong D_3$ symmetries of a triangle

$\Rightarrow |G| = |Orb_x| \cdot |Stab_x| = 48$

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 $g \in G$.

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

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:
$G_{x_i} = \{g \in G : g x_i g^{-1} = x_i\}$.

$|G| = \sum_{i=1}^{m} |C_{x_i}| = \sum_{i=1}^{t} |C_{x_i}| + \sum_{j=1}^{r} |C_{x_j}|$

disjoint union of conj classes

1-elt conj classes: $|Z(G)|$

bigger conj. classes

by orbit-stabilizer: $|C_{x_j}| = \frac{|G|}{|G_{x_j}|}$

where G_{x_j} is the centraliser of x_j in G

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

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:

$$|G| = |Z(G)| + \sum_{j=1}^{r} [G : G_{x_j}]$$

$|G| = p^n$ divisible by p

$G_{x_j} \subset G \Rightarrow |G_{x_j}|$ divides $|G|$

$[G : G_{x_j}] > 1 \Rightarrow$ divisible by p

$\frac{|G|}{|G_{x_j}|} = p^{n-k} > 1$, $p^{k<n}$, p^n

$\Downarrow$

$|Z(G)|$ is divisible by p!

$1 \in Z(G) \Rightarrow |Z(G)| \geq 1 \Rightarrow |Z(G)| \geq p$

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

Cauchy's theorem

Theorem

Let G be a finite abelian group, and p a prime dividing $|G|$. Then G contains an element of order p.

Proof: By minimal criminal. Let G be the smallest counter-example.
$|G|$ is minimal, there is no elt of order p in G, and p divides $|G|$.
Let $g \in G \Rightarrow$ order(g) is not divisible by p (if $g^{kp} = 1 \Rightarrow (g^k)^p = 1$)

$\langle g \rangle \subset G$ subgp $= |\langle g \rangle| =$ order(g), not divisible by $p \Rightarrow |G/\langle g \rangle| = \frac{|G|}{|\langle g \rangle|} < |G|$.

$\Rightarrow p$ divides $|G/\langle g \rangle|$ and $G/\langle g \rangle$ contains an elt of order p., $h \in G/\langle g \rangle$.

$\Rightarrow \exists\, h^p \in \langle g \rangle \Rightarrow h^p = g^s$; let k be the order of g^s

$\Rightarrow (h^p)^k = (g^s)^k = 1 \Rightarrow h^{pk} = 1 \Rightarrow (h^k)^p = 1 \Rightarrow h^k$ has order p.

Cauchy's theorem

Non-abelian case

Cauchy's theorem holds for non-abelian finite groups as well.

Meaning that if p divides $|G|$, then $\exists\, h \in G$ of order p.

[PS 7]: use the class equation of G and the abelian case

$$|G| = \underbrace{|Z(G)|}_{\text{abelian}} + \sum_{j=1}^{r} \frac{|G|}{|G_i|}$$