Abstract Algebra

Week 2 Notes

shaozewxy

August 2022

1.7 Group Actions

The concept of an "action" is important for studying algebraic objects by seeing how it can act on other structures.

Definition of group action

A **group action** of a group G on a set A is a map from $G \times A \to A$. Given $g \in G, a, b \in A$, the action is written as $g \cdot a \to b$. The action needs to satisfy the following properties:

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

2. $\forall a \in A, 1 \cdot a = a$.

Group action defines permutation and homomorphism

Given a group G acting on A. Then $\forall g \in G, \exists \sigma_g : A \to A$ defined by

$$\sigma_g(a) = g \cdot a$$

We observe the following facts:

(i) For each $g \in G, \sigma_g$ is a permutation.

(ii) The map from $G \to S_A$ defined by $g \to \sigma_g$ is a homomorphism.

Proof:

For i, since σ_g maps A to itself, then only NTS σ_g is injective to show σ_g is bijective and therefore a permutation.

Suppose $\exists a, b \in A, \sigma_g(a) = \sigma_a(b)$.

Then $\sigma_g(a) = g{\cdot}a = \sigma_g(b) = g{\cdot}b \to g^{-1}{\cdot}(g{\cdot}a) - g^{-1}{\cdot}(g{\cdot}b) \to 1{\cdot}a = a = 1{\cdot}b = b$.

Therefore σ_g is injective and thus a permutation.

For ii, define $\phi : G \to S_A$ by

$$\phi(g) = \sigma_g$$

then $\forall g, h \in G, \phi(gh) = \sigma_{gh}, \phi(g)\phi(h) = \sigma_g\sigma_h$.

$\forall x \in A, \sigma_{gh}(x) = gh \cdot x = g \cdot h \cdot x = \sigma_g\sigma_h(x)$.

Therefore $\forall g, h \in G, \phi(gh) = \phi(g)\phi(h)$.

The remaining criteria can be easily proved.

The homomorphism above is called the **permutation representation** associated to the given action.

Examples of group actions

1. Define a group action by $\forall g \in G, a \in A, ga = a$.

   This is called a **trivial** action. The associated permutation representation mapping is also trivial as it maps all elements to the identity.

   A group action is said to be **faithful** if distinct elements induce distinct permutations of A, i.e. the associated permutation representation is injective.

   The **kernel** of an action is defined to be $\{g \in G | \forall a \in A, ga = a\}$, i.e. the elements that maps to identity in the associated permutation representaion.

2. The scalar multiplication of a field $\mathbf{F}$ and a vector space V is also an example of group actions with field $\mathbf{F}$ acting on the vector space $\mathbf{F}^n$ defined by

$$\forall a \in \mathbf{F}, v = (v_1, ..., v_n) \in \mathbf{F}^n, av = (av_1, ..., av_n)$$

3. For any non-empty set A the symmetric group S_A acts on A by $\sigma a = \sigma(a)$. The associated permutation association is just the identity map.

4. Each element $\alpha \in D_{2n}$ defined a permuation $\sigma_\alpha \in S_n$ by fixing a labeling of the vertices.

   Therefore D_{2n} defines a group action on $\{1, 2, ..., n\}$ by

$$\forall \alpha \in D_{2n}, i \in \{1, 2, ..., n\}, \alpha \cdot i = \sigma_\alpha(i)$$

5. A finite group of order n is isomorphic to some subgroup of S_n.

   We define a group action of G acting on itself by

$$\forall g, a \in G, g \cdot a = ga$$

   Now we NTS the associated permutation representaion $\pi : G \to S_n$ is injective:

   Suppose $\pi(g) = \pi(h)$, then $\pi(g)g^{-1} = \pi(h)g^{-1} \to hg^{-1} = 1 \to h = g$.

   Therefore π is injective and therefore there is a subgroup in S_n that is isomorphic to G.

2.5 Lattice of Subgroups of a Group

The lattice displays the structure of a group. It is constructed as follow:

- The subgroup 1 is placed at the bottom.
- The group G itself is placed at the top.
- For subgroups A, B there will be a line connecting them if $A \leq B$ and there is no proper subgroup between them.

Drawbacks and Properties of Lattice

For infinite groups, we cannot draw a complete lattice.

Even for some finite groups, the lattice can be very complicated. For example, groups of order 2^n.

However, for these cases, we can draw just part of the lattice which can still be very helpful.

2.4 Subgroups Generated by Subsets of a Group

The concept of given a group G and a subgroup $A \leq G$, is there a unique minimal subgroup that contains A, is a recurring theme.

In vector space this is called a span, and in group this is called **the subgroup generated by** A.

Proposition 8

If $\mathcal{A}$ is a non-empty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup G.

Proof:

Denote

$$K = \bigcap_{H \in \mathcal{A}} H$$

Clearly $1 \in K$.

Given $a, b \in K$. Then $\forall H \in \mathcal{A}, a \in H, b \in H \rightarrow ab \in H$, i.e. $ab \in K$.

Therefore K is a subgroup of G.

Definition of subgroup generated by A

If A is any subset of G, then define

$$\langle A \rangle = \bigcap_{A \subset H \leq G} H$$

This is called **subgroup of G generated by A**.

From Proposition 8 we know that $\langle A \rangle$ is a subgroup, with $\mathcal{A} = \{H \leq G | A \subseteq H\}$.

Since $\forall H, A \subseteq H \rightarrow A \subseteq \langle A \rangle$.

The uniqueness of $\langle A \rangle$ is as follows:

- $\langle A \rangle$ is a subgroup that contains A.
- Any subgroup that contains A also contains $\langle A \rangle$.

Properties of subgroup generated by A

We try to define the same subgroup from bottom up:

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} a_3^{\epsilon_3} ... | n \in \mathbb{Z}, n \geq 0, a_{\in} A, \epsilon_i = \pm 1\}$$

In this definition, a_i need not be distinct.

From this definition we can see how a set is generated from A.

Proposition 9

$$\overline{A} = \langle A \rangle$$

Proof:

First obviously $\overline{A}$ is a subgroup.

Since $\forall a = a_1^{\epsilon_1} a_2^{\epsilon_2} a_3^{\epsilon_3} ... \in \overline{A}, \forall H \in \mathcal{A}, a \in H \to a \in \bigcap_{A \subseteq H \leq G} H \to a \in \langle A \rangle$.

Therefore $\overline{A} \subseteq \langle A \rangle$.

Since clearly $\overline{A}$ is also a subgroup that contains A, then $\langle A \rangle \subseteq \overline{A}$.

Therefore $\overline{A} = \langle A \rangle$.

Limitations of Subgroups Generated by A

If G is abelian, then we could collect the terms in $a_1^{\epsilon_1} a_2^{\epsilon_2} a_3^{\epsilon_3} ...$ to re-define $\langle A \rangle$:

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} ... a_k^{\alpha_k}\}$$

If we further assume that each a_i has finite order d_i, then we can bound the size of $\langle A \rangle$:

$$| \langle A \rangle | \leq d_1 d_2 ... d_k$$

However, if G is non-abelian, then the generated group can be much more complicated.

Let $G = D_8 = \langle r, s \rangle$ and choose $a = s, b = rs, A = \langle a, b \rangle$.

Since $r = rs \cdot s = ba, \to A = G, |A| = |G| = 8$. However, since $|a| = |b| = 2$, it is **impossible** to write all elements in A as $a^\alpha b^\beta$.

The example above shows that for non-aeblian groups, the long product might not be collected. More specifically, the order of a finite group cannot be bounded even if we know the order of all the generating elements of the this group.

In some cases, the group generated by elements of finite orders could even have infinite order:

$$G = GL_2(\mathbb{R}), a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$$

Now both a, b have order 2. But since $ab = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}$, it is clear that $\langle a, b\rangle$ is an infinite subgroup.

2.2 Centralizers and Normalizers, Stablizers and Kernels

Definition of Centralizer

Given set $A \subseteq G$, define

$$\mathbf{C}_G(A) = \{g \in G | \forall a \in A, gag^{-1} = a\}$$

This subset is called the **centralizer** of A in G.

Since $gag^{-1} = a \iff ga = ag$, this is to say $\mathbf{C}_G(A)$ is the set of elements of G which commutes with every elements of A.

Centralizers are Subgroups

Proof:

Obviously $1 \in \mathbf{C}_G(A)$.

Suppose $x, y \in \mathbf{C}_G(A) \to \forall a \in A, xax^{-1} = a, yay^{-1} = a$.

Therefore $xya(xy)^{-1} = xyay^{-1}x^{-1} = xax^{-1} = a$, i.e. $xy \in \mathbf{C}_G(A)$.

This shows that $\mathbf{C}_G(A)$ is a subgroup of G.

Definition of Center

Define $Z(G) = \{g \in G | \forall x \in G, gx = xg\}$, i.e. the set of elements that commutes with all the elements of G. This is called the **center** of G.

Now it is clear that $Z(G) = \mathbf{C}_G(G)$ and therefore $Z(G) \leq G$, and is a special case of centralizer.

Definition of Normalizer

Define $gAg^{-1} = \{gag^{-1} | a \in A\}$. Then the **normalizer** of A in G is

$$N_G(A) = \{g \in G | gAg^{-1} = A\}$$

Note that if $g \in \mathbf{C}_G(A)$ then $\forall g \in A, gag^{-1} = a$ and therefore $C_G(A) \leq N_G(A)$. $N_G(A)$ can be proven to be a subgroup similar to $C_G(A)$.

Examples

1. If G is abelian, then all elements of G commutes and therefore $Z(G) = G$, which also collapses $C_G(A), N_G(A)$ to G.

2. $G = D_8$ the dihedral group, with the usual definition of r, s. Then let $A = \{1, r, r^2, r^3\}$, WTS that $C_{D_8}(A) = A$: Given $sr^i \in D_8, sr^ir^j(sr^i)^{-1} = sr^{i+j}r^{-i}s = sr^js = r^{-j} \neq r^j$.
   Given $r^i \in D_8, r^ir^j(r^i)^{-1} = r^j$.
   Therefore $C_{D_8}(A) = A$

3. In the previous example, we also WTS that $N_{D_8}(A) = D_8$:
   Since $C_G(A) = A \to A \leq N_G(A)$.
   $\forall r^i \in A, sr^is^{-1} = r^{-i}ss^{-1} = r^{-1} \to s \in N_G(A)$.
   Since $r, s \in N_G(A)$ and $N_G(A)$ is a group, this meaqns $N_G(A) = \langle r, s\rangle = G$.

4. The center of D_8 is $\{1, r^2\}$:
   First we can see that for any $A \subseteq G, Z(G) \leq C_G(A) \leq N_G(A)$. Therefore

$Z(G) \leq A = \{1, r, r^2, r^3\}$.

Then given $r^i \in A, r^i s r^j = s r^{-i} r^j$. In order for $r^i s r^i = s r^{-i} r^j = s r^i r^j, \rightarrow$ $r^i = r^{-i} \rightarrow r^i = r^2$.

5. Let $G = S_3, A = \{1, (1\ 2)\}$. WTS $C_{S_3}(A) = N_{S_3}(A) = A$:

   Clearly $A \leq C_{S_3}(A)$. This, along with the fact that $C_{S_3}(A) \leq G$, and LaGrange's theorem, shows that $|C_{S_3}(A)|$ divides $2, 6$.

   i.e. $|C_{S_3}(A)| = 2$ or 6. But since (1 2 3) doesn't commute with (1 2), this means $|C_{S_3}(A)| \neq 6 \rightarrow |C_{S_3}(A)| = 2 \rightarrow C_{S_3}(A) = A$.

   Then NTS $N_{S_3}(A) = A$, since A contains only (1 2) other than 1. This means $\forall \sigma \in N_{S_3}(A), \sigma(1\ 2)\sigma^{-1} = (1\ 2)$ and therefore $\sigma \in C_{S_3}(A)$, i.e. $N_{S_3}(A) = C_{S_3}(A)$.

Stabilizers and Kernels of Group Actions

The normalizer, centralizer of A, and the center of G are all just special cases of results on group actions.

Definition of Stabilizer

Given G a group action on a set S, then fixing an element $s \in S$, the **stabilizer** of s in G is the set

$$G_s = \{g \in G | g \cdot s = s\}$$

Stabilizer is a Subgroup

The proof is obvious and similar to the proof that $C_G(A) \leq G$.

Definition of Kernel

Given G a group acting on a set S. Then the kernel of the action is defined as

$$\{g \in G | \forall s \in S, g \cdot s = s\}$$

similarly,

Kernels are Subgroups

Relations between Centralizers, Normalizers and Stabilizers, Kernels*

If we define $S = \mathcal{P}(G)$, the set of all subsets of G, then we can let G act on S by **conjugation**:

$$\forall g \in G, B \subseteq G, g \cdot B = gBg^{-1}$$

Then in this case, given $A \subseteq G, N_G(A) =$ the stabilizer of A.

Then if we let $N_G(A)$ act on A also by conjugation, i.e.

$$\forall g \in N_G(A), a \in A, g \cdot a = gag^{-1}$$

Note this definition only makes sense when restricting the group to be $N_G(A)$ otherwise gag^{-1} might not be in A.

Then in this case, $C_G(A)$ is just the kernel of this action.

Finally, if we let G act on $S = G$ by conjugation, then $Z(G)$ is just the kernel of this action.