Group action and some applications

Bijan Taeri

October 30,2024

Table of contents

Let X be an algebraic structure and $\mathrm{Aut}(X)$ be the group of the automorphisms of X.

- $\alpha \in \mathrm{Aut}(X)$ if and only if $\alpha : X \to X$ is a permutation which preserves the operations of X.
- $\mathrm{Aut}(X)$ is a subgroup of $\mathrm{Sym}(X)$, the symmetric group on X.

Example

- If X is a set (an algebraic structure with no operations), then $\mathrm{Aut}(X) = \mathrm{Sym}(X)$.

- If K is a group, then $\mathrm{Aut}(K) = \{\alpha \in \mathrm{Sym}(K) \mid \forall x, y \in K,\ \alpha(xy) = \alpha(x)\alpha(y)\}$.

- If V is a vector space, then $\mathrm{Aut}(V) = \mathrm{GL}(V)$, the group of invertible linear transformations of V.

Definition

Let G be a group and X be an algebraic structure. A representation of G is a homomorphism $\varphi : G \longrightarrow \mathrm{Aut}(X)$.

(We say that G acts on X.)

If X is just a set, then φ is called a permutation representation.

If X is a vector space, then φ is called a linear representation.

- For all $g \in G$, $\varphi(g) \in \mathrm{Aut}(X)$.
- $\varphi(1) = \mathrm{id}_X$.
- For all $g, h \in G$, $\varphi(gh) = \varphi(g)\varphi(h)$.

Let $\varphi : G \longrightarrow \mathrm{Sym}(X)$ be a permeation representation of group G on a set X. For $g \in G$, we denote $\varphi(g)$ by φ_g. For all $x \in X$ and $g, h \in G$,

(1) $\varphi_1 = \mathrm{id}_X \implies \varphi_1(x) = x$,

(2) $\varphi_{gh} = \varphi_g \varphi_h \implies \varphi_{gh}(x) = \varphi_g(\varphi_h(x))$.

Thus there is a function $\begin{array}{l} G \times X \longrightarrow X \\ (g, x) \mapsto gx := \varphi_g(x) \end{array}$ such that for all $x \in X$ and $g, h \in G$,

(1') $1x = x$,

(2') $(gh)x = g(hx)$.

In this case we say G acts (from left) on X.

Conversely if there is a function $\begin{aligned} \cdot : G \times X &\longrightarrow X \\ (g,x) &\mapsto g \cdot x \end{aligned}$ such that for all $x \in X$ and $g, h \in G$,

(1') $1 \cdot x = x$,

(2') $(gh) \cdot x = g \cdot (h \cdot x)$,

then for all $g \in G$, the function $\begin{aligned} \lambda_g : X &\to X \\ x &\mapsto g \cdot x \end{aligned}$ is a permutation on X and $\begin{aligned} \lambda : G &\longrightarrow \mathrm{Sym}(X) \\ g &\mapsto \lambda_g \end{aligned}$ is a homomorphism.

Let G acts on a set X and let $\varphi : G \longrightarrow \mathrm{Sym}(X)$ be the corresponding permutation representation.

- $\ker\varphi = \bigcap_{x\in X} \mathrm{stab}(x)$, where $\mathrm{stab}(x) = \{g \in G \mid gx = x\}$.
- The relation $x \sim y \Longleftrightarrow \exists g \in G,\ y = gx$ is an equivalence relation on X.

- The action is called transitive (or G is transitive) if there exists $x \in X$ such that $X = \mathrm{orb}(x)$.
- The action is called faithful (or G is faithful) if $\ker\varphi = \{1\}$.
- The action is called regular (or G is regular) if it is faithful and transitive.

Orbit-Stabilizer Theorem

$|\mathrm{orb}(x)| = |G : \mathrm{stab}(x)|$. In particular if G is finite, then $|\mathrm{orb}(x)|$ divides $|G|$.

Theorem

If X is finite, then $|X| = |X_f| + \sum_{i=1}^{k} |G : \mathrm{stab}(x_i)|$, where X_f is the set of orbits of size 1, and $\{\mathrm{stab}(x_1), \ldots, \mathrm{stab}(x_k)\}$ is the set of all orbits of size ≥ 2. In particular if G is a finite p-group, then $|X| \equiv |X_f| \pmod{p}$.

Example (Left regular action)

A group G acts on $X = G$, by left multiplication. The corresponding permutation representation is $\begin{array}{c} L : G \longrightarrow \mathrm{Sym}(G) \\ g \mapsto L_g \end{array}$,

where $\begin{array}{c} L_g : G \to G \\ x \mapsto gx \end{array}$

The action is faithful and $G \cong L_G = \{L_g \mid g \in G\} \leq \mathrm{Sym}(G)$. (Cayley, 1854)

This action is transitive, since for all $x, y \in G$,

$$y = (yx^{-1})x = L_{yx^{-1}}(x).$$

Vertex transitive

Let $\Gamma = (V, E)$ be a simple graph. Then

$$\mathrm{Aut}(\Gamma) = \{\alpha \in \mathrm{Sym}(V) \mid \forall x, y \in V,\ x \sim y \Longleftrightarrow \alpha(x) \sim \alpha(y)\}$$

acts on V naturally: $\alpha x = \alpha(x)$.

- Γ is called vertex transitive if $\mathrm{Aut}(\Gamma)$ acts transitively on V.
- If Γ is vertex transitive, then Γ is regular (all vertices have the same degree).

An easy way to construct vertex transitive graphs

Cayley graph (Cayley, 1878)

Let G be a group and $S \subseteq G$, such that $S = S^{-1}$ and $1 \notin S$. The Cayley graph $\Gamma := \mathrm{Cay}(G, S)$ is a simple graph and defined as follows:

$$V(\Gamma) = G \quad \text{and} \quad E(\Gamma) = \{(g, gs) \mid s \in S\}.$$

$$g, h \in G, \quad g \sim h \Longleftrightarrow g^{-1}h \in S.$$

$\mathrm{Cay}(G, S)$ is a simple graph $|S|$-regular and it is connected if and only if $G = \langle S \rangle$.

Theorem (Sabidussi, 1958)

A graph Γ is a Cayley graph if and only if $\mathrm{Aut}(\Gamma)$ contains a regular subgroup.

Let $\Gamma = \mathrm{Cay}(G, S)$. For all $g, x, y \in G$

$$\begin{aligned} x \sim y &\iff x^{-1}y \in S \iff (gx)^{-1}gy \in S \iff gx \sim gy \\ &\iff L_g(x) \sim L_g(y) \end{aligned}$$

Thus $G \cong L_G = \{L_g \mid g \in G\} \leq \mathrm{Aut}(\Gamma)$. Thus $\mathrm{Aut}(\Gamma)$ contains a regular subgroup. (In particular $\mathrm{Cay}(G, S)$ is vertex transitive.)

Conversely if a group G acts regularly on the vertices of a graph Γ, then Γ is the Cayley graph of G relative to some subset of S of G, with $S = S^{-1}$ and $1 \notin S$.

Example (A generalization of the left regular action)

Let $H \leq G$. Then G acts on $X = \{xH \mid x \in G\}$, the set of left cosets of H in G, by left multiplication. The corresponding permutation representation is $\begin{array}{c} \rho : G \longrightarrow \mathrm{Sym}(X) \\ g \mapsto \rho_g \end{array}$, where

$$\begin{aligned} \rho_g : X &\to X \\ xH &\mapsto g(xH) = gxH. \end{aligned}$$

We have $\mathrm{stab}(xH) = xHx^{-1}$ and $\ker\rho = H_G = \bigcap_{x \in G} xHx^{-1}$, the core of H in G, so G/H_G is (isomorphic to) a subgroup of $\mathrm{Sym}(X)$.

Example (Conjugation action)

A group G acts on $X = G$, by conjugation. The corresponding (automorphism) representation is $\begin{aligned} \tau : G &\longrightarrow \mathrm{Aut}(G) \\ g &\mapsto \tau_g \end{aligned}$, where

$$\begin{aligned} \tau_g : G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$$

- The kernel if the action is $Z(G) = \{g \in G \mid \forall x,\ xg = gx\}$, the center of G and $G/Z(G) \cong \mathrm{Im}(\tau) = \mathrm{Inn}(G)$.
- The class equation is $|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(x_i)|$.
- If G is a finite p-group, then $|G| \equiv |Z(G)| \pmod{p}$ and so $Z(G)$ is non-trivial.

Sylow's First Theorem (Sylow, 1872)

Let G be a finite group and $|G| = p^n m$, where p is prime and $p \nmid m$. Then there exists a subgroup P of G such that $|P| = p^n$.

Thus $\mathrm{Syl}_p(G)$, the set of Sylow p-subgroups of G is non-empty.

$$P \in \mathrm{Syl}_p(G) \Longleftrightarrow P \text{ is a } p-\text{subgroup and } p \nmid |G : P|.$$

Sylow's Second Theorem

Let G be a finite group and $P, H \in \mathrm{Syl}_p(G)$. Then there exists $g \in G$ such that $H = gPg^{-1}$. Hence the action of G on $\mathrm{Syl}_p(G)$, by conjugation, is transitive.

Proof. Put $X = \{xP \mid x \in G\}$. Thus p does not divide $|X| = |G : P|$. Now H acts on X: $h(xP) = hxP$.

Since $|X| \equiv |X_f| \pmod{p}$, $|X_f| \neq 0$ and there exists $xP \in X$ such that $\mathrm{orb}(xP) = \{xP\}$. Thus

$$\begin{aligned} \forall h \in H, hxP = xP &\iff \forall h \in H, x^{-1}hx \in P \\ &\iff H \leq xPx^{-1} \\ &\iff H = xPx^{-1}. \end{aligned}$$

Sylow's Third Theorem

Let G be a finite group. $n_p \equiv 1 \pmod{p}$, where $n_p = |\mathrm{Syl}_p(G)|$.

Proof. Put $P \in \mathrm{Syl}_p(G)$. Then P acts on $X = \mathrm{Syl}_p(G)$ by conjugation. It is easy to see that $X_f = \{P\}$ and so $|X_f| = 1$. Now since $|X| \equiv |X_f| \pmod{p}$, we have $n_p \equiv 1 \pmod{p}$.

(Internal) Semi-direct product

Let K be a normal subgroup of G and $H \leq G$ such that $G = KH$ and $H \cap K = \{1\}$. Then H acts on K by conjugation. The corresponding representation is $\begin{array}{c}\tau : H \longrightarrow \mathrm{Aut}(K) \\ h \mapsto \tau_h\end{array}$, where

$$\tau_h : K \to K$$
$$k \mapsto k^h := hkh^{-1}$$

The multiplication in G:

$$(k_1h_1)(k_2h_2) = k_1h_1k_2h_1^{-1}h_1h_2 = k_1\tau_{h_1}(k_2)h_1h_2 = (k_1k_2^{h_1})(h_1h_2),$$

We say that G is a semi-direct product of K by H and write $G = K \rtimes H = K \rtimes_\tau H$.

(External) Semi-direct product

Let H and K be arbitrary groups such that H acts K. Let the corresponding representation be $\begin{array}{c}\varphi : H \longrightarrow \mathrm{Aut}(K)\\ h \mapsto \varphi_h\end{array}$.

Then we define a multiplication in $G = K \times H$ (denote $\varphi_h(k)$ by k^h)

$$(k_1, h_1)(k_2, h_2) = (k_1\varphi_{h_1}(k_2), h_1h_2) \quad \Big(= (k_1k_2^{h_1}, h_1h_2)\Big).$$

Then G is a group. We call it semi-direct product of K by H and write $G = K \rtimes_\varphi H$.

It is easy to see that G is the internal semi-direct product of $\overline{K} = \{(k, 1) \mid k \in K\}$ by $\overline{H} = \{(1, h) \mid h \in H\}$ and $G = \overline{K} \rtimes_\tau \overline{H}$.

Groups of order pq

Let $H = \langle h \rangle \cong \mathbb{Z}_3$ and $K = \langle k \rangle \cong \mathbb{Z}_7$. Then $\mathrm{Aut}(K) \cong \mathbb{Z}_6$ and H acts on K: $\begin{array}{c} \varphi : H \longrightarrow \mathrm{Aut}(K) \\ h \mapsto \varphi_h \end{array}$, $\begin{array}{c} \varphi_h : K \longrightarrow K \\ k \mapsto k^2 \end{array}$.

The semi direct product

$$K \rtimes H = \langle h, k \mid h^3 = 1,\ k^7 = 1, \overbrace{hkh^{-1}}^{\varphi_h(k)} = k^2 \rangle,$$

of K by H is the unique non abelian group of order 21.

More generally every non-abelian group of order pq, where p and q are primes, $p < q$, and $q \equiv 1 \pmod p$, is of the form

$$\langle h, k \mid h^p = 1,\ k^q = 1, hkh^{-1} = k^r \rangle,$$

where $r \not\equiv 1 \pmod q$ and $r^p \equiv 1 \pmod q$.

Let K be a subgroup of $\mathrm{Aut}(G)$. Then K acts naturally on G: $\forall\alpha \in K$, $\forall x \in G$, $\alpha x = \alpha(x)$. Thus we can form the semi-direct product

$$W = G \rtimes K = \{x\alpha \mid x \in G,\ \alpha \in K\},$$

with respect to this action. W is called the relative holomorph.

The holomorph of G is

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{x\alpha \mid x \in G,\ \alpha \in \mathrm{Aut}(G)\}.$$

$$(x\alpha)(y\beta) = x\alpha(y)\alpha\beta,$$

Generalized dihedral group

Let A be an abelian group. Assume that there exists $a \in A$ with $a^2 \neq 1$. Then $\eta : a \mapsto a^{-1}$ is a non-identity automorphism and $\eta^2 = 1$. We can form the relative holomorph

$$\mathrm{Dih}(A) = A \rtimes \langle \eta \rangle = \{a\eta^j \mid a \in A,\ j \in \{0,1\}\},$$

the generalized dihedral group.

$$(a\eta)(b\eta) = a\eta(b)\eta\eta = ab^{-1}$$

$$(a\eta)^2 = (a\eta)(a\eta) = a\eta(a)\eta\eta = aa^{-1} = 1$$

$$D_{2n} = Dih(\mathbb{Z}_n), \qquad D_\infty = Dih(\mathbb{Z})$$

Let G be a group. Let H be a group acting on a set X. Then H acts on

$$G^X = \{f \mid f : X \to G\}$$

of all sequence of elements of G indexed by X, which is group $(fg(x) = f(x)g(x))$. For all $h \in H$ and $f \in G^X$, $f^h := h \cdot f \in G^X$, where

$$f^h(x) = (h \cdot f)(x) = f(h^{-1}x) \ \left(f = (g_x)_{x \in X},\ h \cdot f = (g_{h^{-1}x})_{x \in X}\right).$$

The semi-direct product $W = G \wr H = G^X \rtimes H$ of G^X by H is called, the wreath product of G and H.

$$(fh)(gk) = fg^h hk$$

Let G be any group. The group $\mathrm{Sym}(n)$ acts on $X = \{1, 2, \ldots, n\}$. Now

$$G^X = \{(g_1, \ldots, g_n) \mid g_i \in G\}$$

and for all $\sigma \in \mathrm{Sym}(n)$,

$$\sigma \cdot (g_1, \ldots, g_n) = (g_{\sigma^{-1}(1)}, \ldots, g_{\sigma^{-1}(n)}).$$

$$W = G \wr S_n = G^X \rtimes S_n = \{(g_1, \ldots, g_n)\sigma \mid g_i \in G,\ \sigma \in S_n\}$$

$$\begin{aligned}(a_1, \ldots, a_n)\alpha(b_1, \ldots, b_n)\beta &= (a_1, \ldots, a_n)(b_1, \ldots, b_n)^{\alpha}\alpha\beta \\ &= (a_1 b_{\alpha^{-1}(1)}, \ldots, a_n b_{\alpha^{-1}(n)})\alpha\beta\end{aligned}$$

Theorem (Frucht, 1949)

Let a finite graph Γ be the disjoint union of n copies of a connected graph H. Then

$$\mathrm{Aut}(\Gamma) = \mathrm{Aut}(H) \wr \mathrm{Sym}(n).$$

THANK YOU