Group actions

Tuesday, June 29, 2021 3:29 PM

As it has been mentioned earlier, group theory has been developed to study symmetries of objects. Our meta-example for groups is $\mathrm{Sym}(X)$ where X is an "object". Now starting with a group G, we would like to see if it can be view as symmetries of an object. The easiest object is of course just a set X. So having a group G and a set X, we would like to permute elements of X in a way compatible with group operation of G. This brings us to the definition of group actions.

<u>Def.</u> Suppose $(G,\cdot)$ is a group and X is a non-empty set. We say G acts on X via $*: G\times X \to X$ if

(a) $\forall x\in X$, $\quad e_G * x = x$,

(b) $\forall g_1, g_2 \in G$, $x\in X$, $\quad g_1 * (g_2 * x) = (g_1\cdot g_2) * x$.

<u>Remark</u>. We often use $\cdot$ to denote both the group action and the group operation. Because of (b), it should not cause a serious problem; but you should be aware of this.

Examples of group actions

Tuesday, June 29, 2021 3:29 PM

When a group G acts on a set X via $*$ we write

$$G \underset{*}{\curvearrowright} X \quad \text{or simply} \quad G \curvearrowright X.$$

<u>Ex.</u> Suppose X is a non-empty set. Then the symmetric group S_X acts on X via $*: S_X \times X \to X$, $\sigma * x := \sigma(x)$

(we apply σ to x; or we say σ acts on x.)

<u>Pf.</u> • $\mathrm{id} * x = \mathrm{id}(x) = x$ for every $x \in X$

• $\sigma_1 * (\sigma_2 * x) = \sigma_1 * (\sigma_2(x)) = \sigma_1(\sigma_2(x))$

$= (\sigma_1 \circ \sigma_2)(x) = (\sigma_1 \circ \sigma_2) * x.$ ∎

<u>Ex.</u> Suppose $(G, \cdot)$ is a group. Then $G \curvearrowright G$ via left multiplication; that means $g * x := g \cdot x$.

<u>Pf.</u> • $e_G * x = e_G \cdot x = x$ (neutral element)

• $g_1 * (g_2 * x) = g_1 * (g_2 \cdot x) = g_1 \cdot (g_2 \cdot x)$

$= (g_1 \cdot g_2) \cdot x$ (associative)

$= (g_1 \cdot g_2) * x.$ ∎

<u>Ex.</u> Suppose $(G, \cdot)$ is a group. Then $G \curvearrowright G$ via conjugation; that means $g * x := g \cdot x \cdot g^{-1}$.

Group actions and permutations

Tuesday, June 29, 2021 3:29 PM

<u>Pf.</u> • $e_G * x = e_G \cdot x \cdot e_G^{-1} = x$

• $g_1 * (g_2 * x) = g_1 * (g_2 \cdot x \cdot g_2^{-1})$

$$= g_1 \cdot (g_2 \cdot x \cdot g_2^{-1}) \cdot g_1^{-1}$$

$$= (g_1 \cdot g_2) \cdot x \cdot (g_2^{-1} \cdot g_1^{-1})$$

$$= (g_1 \cdot g_2) \cdot x \cdot (g_1 \cdot g_2)^{-1}$$

$$= (g_1 \cdot g_2) * x \qquad \blacksquare$$

Suppose $G \underset{*}{\curvearrowright} X$. Then, for every $g \in G$, $x \mapsto g * x$ is a function from X to X. Let's call this function σ_g.

So $\sigma_g : X \to X$, $\sigma_g(x) = g * x$. Notice that

$\sigma_{e_G}(x) = e_G * x = x$, and so $\sigma_{e_G} = id$. and

$\forall g_1, g_2 \in G$, $(\sigma_{g_1} \circ \sigma_{g_2})(x) = \sigma_{g_1}(\sigma_{g_2}(x))$

$$= \sigma_{g_1}(g_2 * x)$$

$$= g_1 * (g_2 * x)$$

$$= (g_1 \cdot g_2) * x = \sigma_{g_1 \cdot g_2}(x).$$

In particular, $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{g \cdot g^{-1}} = \sigma_{e_G} = id$ and similarly

$\sigma_{g^{-1}} \circ \sigma_g = id$. Therefore $\forall g \in G$, $\sigma_g : X \to X$ is a bijection.

Group actions and permutations

Tuesday, June 29, 2021 3:29 PM

This means if $G \curvearrowright_{*} X$ and $\sigma_g : X \to X$, $\sigma_g(x) := g * x$,

then $\sigma_g \in S_X$.

<u>Theorem</u>. Suppose $G \curvearrowright_{*} X$. Then

$$f : G \to S_X, \quad f(g) := \sigma_g$$

is a group homomorphism.

<u>Pf.</u> • We have already proved that for every $g \in G$, $\sigma_g \in S_X$,

and so f is well-defined.

• $\forall g_1, g_2$, $f(g_1 \cdot g_2) = \sigma_{g_1 \cdot g_2} = \sigma_{g_1} \circ \sigma_{g_2} = f(g_1) \circ f(g_2)$,

(we showed this earlier)

and so f is a group homomorphism. ∎

<u>Ex.</u> If $G \curvearrowright_{*} X$ and H is a subgroup of G, then $H \curvearrowright_{*} X$.

<u>Pf.</u> Since H is a subgroup of G, $e_H = e_G$. Hence for every

$x \in X$, $e_H * x = e_G * x = x$. For every $h_1, h_2 \in H$,

$h_1 * (h_2 * x) = (h_1 \cdot h_2) * x$ (as h_i's are in G and $H \leq G$.) ∎

• Suppose $\sigma \in S_n$. Then $\langle \sigma \rangle \curvearrowright \{1, 2, \ldots, n\}$. This is

because $S_n \curvearrowright \{1, 2, \ldots, n\}$ via $\tau * i := \tau(i)$. Let's recall

Group actions and orbits

Tuesday, June 29, 2021 3:29 PM

that to understand cycle decomposition of σ, we follow the flow, and that means for every $a \in \{1, 2, \ldots, n\}$, we considered

$$\begin{array}{c} a \to \sigma(a) \to \sigma^2(a) \to \cdots \to \sigma^{m-1}(a) \\ \uparrow\!\underline{\hspace{12em}}\! \lrcorner \end{array}$$

We can interpret this in terms of the action of $\langle\sigma\rangle$ on $\{1, \ldots, n\}$:

$$\begin{array}{c} a \to \sigma * a \to \sigma^2 * a \to \cdots \to \sigma^{m-1} * a \\ \uparrow\!\underline{\hspace{12em}}\! \lrcorner \end{array}$$

Hence support of this cycle is

$$\{\sigma^i * a \mid i \in \mathbb{Z}\}.$$

All the points that we can get to, using the action of $\langle\sigma\rangle$ on $\{1, 2, \ldots, n\}$. We can interpret this as saying: if we only symmetries that are induced by $\langle\sigma\rangle$, what points are similar to a? The answer is $\{\sigma^i * a \mid i \in \mathbb{Z}\}$. This brings us to the definition of G-orbits of an action $G \curvearrowright_* X$.

Def. Suppose $G \curvearrowright_* X$, we say $x, y \in X$ are G-similar and write $x \sim y$ if $\exists g \in G, y = g * x$. The set of all the points that are G-similar to x is denoted by

Group actions and orbits

Tuesday, June 29, 2021 3:29 PM

$G*x$. We call $G*x$ the G-orbit of x, we sometimes denote $G*x$ by $\mathcal{O}_x$.

<u>Theorem</u>. Suppose $G \curvearrowright_* X$. Then

(1) G-similarity is an equivalent relation.

(2) The G-orbit $G*x$ of x is the equivalent class of x for the G-similarity relation.

(3) The set $\{G*x \mid x\in X\}$ of G-orbits is a partition of X.

<u>Pf.</u> (1) We have to show that $\sim_G$ is reflexive, symmetric, and transitive.

<u>Reflexive</u>. $x \sim_G x$? $\quad x \sim e_G * x \Rightarrow x \sim x$

<u>Symmetric</u>. $x \sim_G y \overset{?}{\Rightarrow} y \sim_G x$.

$$x \sim_G y \Rightarrow \exists g\in G,\ y = g*x$$

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

$$= e_G * x = x$$

$$\Rightarrow y \sim_G x.$$

Orbits and partition

Tuesday, June 29, 2021 3:29 PM

Transitive. $\left.\begin{array}{l} x\sim_G y \\ y\sim_G z \end{array}\right\} \overset{?}{\Longrightarrow} x\sim_G z.$

$\left.\begin{array}{l} x\sim_G y \Rightarrow \exists g\in G,\ y=g*x \\ y\sim_G z \Rightarrow \exists g'\in G,\ z=g'*y \end{array}\right\} \Rightarrow$

$z=g'*y=g'*(g*x)=(g'\cdot g)*x \Rightarrow$

$x\sim_G z.$

(2) Let $[x]_{\sim_G}$ be the equivalent class of x with respect to $\sim_G$. This means $[x]_{\sim_G}=\{y\in X \mid y\sim_G x\}$. We want to show $[x]_{\sim_G}=G*x$.

$y\in[x]_{\sim_G} \Rightarrow y\sim_G x \Rightarrow x\sim_G y$

$\Rightarrow \exists g\in G,\ y=g*x$

$\Rightarrow y\in G*x.$ Hence $[x]_{\sim_G}\subseteq G*x.$ (I)

$z\in G*x \Rightarrow \exists g\in G,\ z=g*x \Rightarrow x\sim z$

$\Rightarrow z\sim x \Rightarrow z\in[x]_{\sim_G}$

Hence $G*x\subseteq[x]_{\sim_G}.$ (II)

By (I) and (II), $[x]_{\sim_G}=G*x.$

Orbits and partition

Tuesday, June 29, 2021 3:29 PM

(3) We want to show that $\{G*x \mid x\in X\}$ is a partition of X. By the 2nd part $\{G*x \mid x\in X\} = \{[x]_{\sim_G} \mid x\in X\}$.
Since $\sim_G$ is an equivalent relation on X, $\{[x]_{\sim_G} \mid x\in X\}$ is a partition of X. This completes the proof. ∎

<u>Def.</u> Suppose $G \curvearrowright_* X$. The set $\{G*x \mid x\in X\}$ of all G-orbits is denoted by $G\backslash X$.
Since $G\backslash X$ is a partition of X, we have

$$|X| = \sum_{G*x\in G\backslash X} |G*x|.$$

Let's go over some of our group action examples and discribe their orbits.

- $S_n \curvearrowright \{1,2,\ldots,n\}$. For every a, the transposition $(1,a)$ sends 1 to a. Hence $(1,a)*1=a$, which means a is in the S_n-orbit of 1. For every point a, $1 \sim_{S_n} a$. Therefore there is only <u>one</u> S_n-orbit and $S_n\backslash\{1,2,\ldots,n\}$ has only <u>one</u> element.

Examples of orbits

Tuesday, June 29, 2021 3:29 PM

We say G acts transitively on X if there is only one G-orbit; that means for every $x, y \in X$, there is $g \in G$ such that

$$y = g * x.$$

(Every point is G-similar to another point of X.)

Ex. $S_n \curvearrowright \{1, 2, \dots, n\}$, $\sigma * a := \sigma(a)$ is a transitive action.

Ex. $G \curvearrowright G$ by left multiplication; that means $g * x := g \cdot x$.

For every $y \in G$, $(y \cdot x^{-1}) * x = (y \cdot x^{-1}) \cdot x = y$, and so $y \in G \cdot x$. Hence $G \curvearrowright G$ by left multiplication is transitive.

Ex. $G \curvearrowright G$ by conjugation; that means $g * x := g \cdot x \cdot g^{-1}$.

Then the G-orbit $G * x$ of x is $\{g * x \mid g \in G\}$, and so

$$G * x = \{g \cdot x \cdot g^{-1} \mid g \in G\}$$

is the set of all conjugates of x. The set of all the conjugates of x is called the conjugacy class of x, and it is denoted by $Cl(x)$. Since $\{G * x \mid x \in G\}$ is a partition of G, we conclude that conjugacy classes form a partition of G.

Cosets of a subgroup

Tuesday, June 29, 2021 3:29 PM

<u>Ex.</u> Suppose $(G,\cdot)$ is a group and H is a subgroup of G.

Then $H \curvearrowright G$ by left multiplication. This is the case because $G \curvearrowright G$ by left multiplication and H is a subgroup of G. The H-orbit of x is

$$H * x := \{h * x \mid h \in H\} = \{h \cdot x \mid h \in H\}.$$

In this case the H-orbit is denoted by $H\cdot x$. Since the H-orbits form a partition of G, we conclude that

$$H\backslash G = \{H\cdot x \mid x \in G\} \text{ is a partition of } G.$$

$H\cdot x$ is called a right coset of H.

<u>Theorem.</u> Suppose $(G,\cdot)$ is a group and H is a subgroup of G.

(1) $H\cdot x = H\cdot y \iff x\cdot y^{-1} \in H$

(2) $H \to H\cdot x$, $h \mapsto h\cdot x$ is a bijection and so $|H| = |H\cdot x|$.

(3) If G is a finite group, then $|G| = |H\backslash G|\,|H|$.

<u>Pf.</u> (1) Let's recall that $H\cdot x = H * x$ is the H-orbit of x and $H*x$ is the equivalent class of x under H-similarity relation; that means $H*x = [x]_{\sim_H}$. Therefor $H\cdot x = H\cdot y$

implies $[x]_\sim = [y]_\sim$. We have seen that two equivalent classes $[x]_\sim$ and $[y]_\sim$ are equal exactly when $x \sim y$. Thus

$H\cdot x = H\cdot y \iff y$ is H-similar to x

which means $y = h * x = h\cdot x$ for some $h \in H$

$\iff y\cdot x^{-1} = h$ for some $h \in H$.

$\iff y\cdot x^{-1} \in H$.

(Because the above proof many parts involving earlier results, let's see another argument:

$H\cdot x = H\cdot y \implies e_G\cdot x \in H\cdot y \implies x \in H\cdot y$

$\implies \exists h \in H,\ x = h\cdot y$

$\implies \exists h \in H,\ x\cdot y^{-1} = h$

$\implies x\cdot y^{-1} \in H$.

Suppose $x\cdot y^{-1} = h_0 \in H$. We want to show $H\cdot x = H\cdot y$.

To show equality of these two sets, we show that every element of $H\cdot y$ is in $H\cdot x$, and vice versa.

$z \in H\cdot y \implies \exists h \in H,\ z = h\cdot y$

Cosets of a subgroup

Tuesday, June 29, 2021 3:29 PM

$$\Rightarrow z = h\cdot y = h\cdot h_0^{-1}\cdot h_0\cdot y$$
$$= \underbrace{(h\cdot h_0^{-1})}_{\text{in } H}\cdot x\cdot \underbrace{y^{-1}\cdot y}_{e_G}$$
$$= \underbrace{(h\cdot h_0^{-1})}_{\text{in } H}\cdot x \in H\cdot x.$$

. $z\in H\cdot x \Rightarrow \exists h\in H,\ z = h\cdot x$

$$\Rightarrow z = h\cdot h_0\cdot h_0^{-1}\cdot x$$
$$= \underbrace{(h\cdot h_0)}_{\text{in } H}\cdot \underbrace{(x\cdot y^{-1})^{-1}}_{y\cdot x^{-1}}\cdot x$$
$$= \underbrace{(h\cdot h_0)}_{\text{in } H}\cdot y \in H\cdot y. \qquad)$$

(2) We want to show $f: H\to H\cdot x,\ f(h) := h\cdot x$ is a bijection. Since every element of $H\cdot x$ is of the form $h\cdot x$ for some $h\in H$, f is surjective (and well-defined). Next we discuss why f is injective:

$$f(h_1) = f(h_2) \Rightarrow h_1\cdot x = h_2\cdot x$$
$$\Rightarrow h_1 = h_2 \text{ by the cancellation law}$$

Hence f is injective, and so it is bijective.

Cosets of a subgroup and Lagrange's theorem

Tuesday, June 29, 2021 3:29 PM

Since $H\backslash G$ is a partition of G, we have

$$|G| = \sum_{H\cdot x \in H\backslash G} |H\cdot x|. \qquad (I)$$

By the previous part, $|H\cdot x| = |H|$ for every $x \in G$. Hence by (I), we have

$$|G| = \sum_{H\cdot x \in H\backslash G} |H| = |H\backslash G|\,|H|. \qquad \blacksquare$$

Def. Suppose H is a subgroup of G. The cardinality $|H\backslash G|$ of the set of all right H-cosets is called the index of H in G, and it is denoted by $[G:H]$.

Theorem (Lagrange) Suppose H is a subgroup of G. Then

$$|G| = [G:H]\,|H|;$$

in particular $|H| \mid |G|$.

Here is an important corollary of Lagrange's theorem.

Corollary. Suppose G is a finite group. Then, for every $g \in G$, $o(g) \mid |G|$, and so $g^{|G|} = e_G$.

Pf. We know that $|\langle g\rangle| = o(g)$. By Lagrange's theorem,

Lagrange's theorem and Euler's theorem

Tuesday, June 29, 2021 3:29 PM

$|\langle g\rangle| \mid |G|$, and so $o(g) \mid |G|$.

We know that if $o(g)=d$, then

$$g^m = e_G \iff d \mid m.$$

Because $o(g) \mid |G|$, we deduce that $g^{|G|} = e_G$. ∎

Here is a nice application of Lagrange's theorem to classical number theory.

<u>Theorem</u> (Euler) Suppose n is a positive integer, $a \in \mathbb{Z}$, and $\gcd(a,n)=1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

<u>Pf.</u> Consider the group $(\mathbb{Z}_n^\times, \cdot)$. Since $\gcd(a,n)=1$, $[a]_n \in \mathbb{Z}_n^\times$. Hence $[a]_n^{|\mathbb{Z}_n^\times|} = [1]_n$. Let's recall that $|\mathbb{Z}_n^\times| = \phi(n)$. Therefore $[a]_n^{\phi(n)} = [1]_n$. Hence $[a^{\phi(n)}]_n = [1]_n$, which implies that $a^{\phi(n)} \equiv 1 \pmod{n}$. ∎

<u>Theorem (Fermat's little theorem)</u> Suppose p is prime. Then for every $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

<u>Pf.</u> If $a \equiv 0 \pmod{p}$, then $a^p \overset{p}{\equiv} 0 \equiv a$. If $a \overset{p}{\not\equiv} 0$, then $\gcd(a,p)=1$, and so $a^{\phi(p)} \equiv 1 \pmod{p}$. Since $\phi(p)=p-1$,

Examples of index of subgroups

Tuesday, June 29, 2021 3:29 PM

$a^{p-1} \equiv 1 \pmod p$ if $a \not\equiv 0$. Multiply both sides by a, we obtain $a^p \equiv a \pmod p$. ∎

<u>Ex.</u> Find $|A_n|$ and $[S_n : A_n]$ for $n \geq 2$.

<u>Solution.</u> <u>Claim</u> If σ is even, then $A_n \sigma = A_n$, and if σ is odd, then $A_n \sigma = A_n (1,2)$.

<u>Pf of claim</u>. Let's recall that $Hx = Hy \Leftrightarrow xy^{-1} \in H$.

- $\sigma \in A_n \Rightarrow \sigma \cdot id^{-1} \in A_n \Rightarrow A_n \sigma = A_n\, id \Rightarrow A_n \sigma = A_n$.
- σ is odd $\Rightarrow \operatorname{sgn}(\sigma) = -1$

$$\Rightarrow \operatorname{sgn}(\sigma(1,2)) = \operatorname{sgn}(\sigma)\operatorname{sgn}(1,2)$$

$$= (-1)(-1) = 1$$

$$\Rightarrow \sigma(1,2) \in A_n$$

$$\Rightarrow \sigma (1,2)^{-1} \in A_n \qquad (\text{as } (1,2)^{-1} = (1,2))$$

$$\Rightarrow A_n \sigma = A_n (1,2).$$

Therefore $A_n \backslash S_n = \{A_n \sigma \mid \sigma \in S_n\} = \{A_n, A_n(1,2)\}$, which implies $|A_n \backslash S_n| = 2$. Thus $[S_n : A_n] = 2$. By Lagrange's thm, $|S_n| = [S_n : A_n]\,|A_n|$. We deduce that $|A_n| = \frac{n!}{2}$. ∎

Examples of index of subgroups

Tuesday, June 29, 2021 3:29 PM

Ex. Suppose D_{2n} is the dihedral group and $\sigma, \tau \in D_{2n}$ are

$\sigma: \mathbb{Z}_n \to \mathbb{Z}_n$, $\sigma(x) = x + [1]_n$ and $\tau: \mathbb{Z}_n \to \mathbb{Z}_n$, $\tau(x) = -x$.

Find $[D_{2n} : \langle \sigma \rangle]$ and $[D_{2n} : \langle \tau \rangle]$.

Solution. • Notice that $\sigma^m(x) = x + [m]_n$, and so $\sigma^m = id.$ exactly when $n \mid m$. Hence $o(\sigma) = n$. Therefore $|\langle \sigma \rangle| = n$.

Thus $[D_{2n} : \langle \sigma \rangle] = \dfrac{|D_{2n}|}{|\langle \sigma \rangle|} = \dfrac{2n}{n} = 2$.

• Notice that $\tau^2 = id.$, and so $o(\tau) = 2$. Thus $|\langle \tau \rangle| = 2$.

Therefore $[D_{2n} : \langle \tau \rangle] = \dfrac{|D_{2n}|}{|\langle \tau \rangle|} = \dfrac{2n}{2} = n$. $\blacksquare$