Group actions

Tuesday, June 29, 2021 3:29 PM

Let's recall the basics of group actions. Suppose G is a group and X is a non-empty set. We say G acts on X via $*$ if $G\times X \to X$, $(g,x)\mapsto g*x$ is a function with the following properties: (1) $\forall x\in X$, $e_G * x = x$,

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

We say y is G-similar to x and write $x\sim_G y$ if $y=g*x$ for some $g\in G$. We proved that $\sim_G$ is an equivalent relation, and $[x]_{\sim_G}=\{g*x \mid g\in G\}$. We let $G*x := \{g*x \mid g\in G\}$ and call it the G-orbit of x. We deduce that $\{G*x \mid x\in X\}$ is a partition of X, and $G*x = G*y \Leftrightarrow x\sim_G y \Leftrightarrow \exists g\in G,\ y=g*x$. The set of all G-orbits is denoted by ${}_G\backslash X$. When X is finite, we have $|X| = \sum_{G*x\in {}_G\backslash X} |G*x|$. This is the case as ${}_G\backslash X$ is a partition of X. Next we want to understand $|G*x|$. To answer this question it is important to study elements of g that do not move x. We say they

Stabilizer subgroups

Tuesday, June 29, 2021 3:29 PM

stabilize x.

Lemma. Let $G_x := \{ g \in G \mid g * x = x \}$. Then G_x is a subgroup of G. (G_x is called the stabilizer subgroup of G with respect to x.)

Pf. We use the subgroup criterion. We start by discussing why $e_G \in G_x$. We have that $e_G * x = x$, and so $e_G \in G_x$.

Next we have to show $g_1, g_2 \in G_x \Rightarrow g_1 \cdot g_2^{-1} \in G_x$.

$$g_2 \in G_x \Rightarrow g_2 * x = x \Rightarrow g_2^{-1} * (g_2 * x) = g_2^{-1} * x$$

$$\Rightarrow (g_2^{-1} \cdot g_2) * x = g_2^{-1} * x \Rightarrow e_G * x = g_2^{-1} * x$$

$$\Rightarrow x = g_2^{-1} * x. \qquad \text{(I)}$$

Letting g_1 act on both sides of (I) we obtain that

$$g_1 * x = g_1 * (g_2^{-1} * x). \qquad \text{(II)}$$

- $g_1 \in G_x \Rightarrow g_1 * x = x$ (III)
- $g_1 * (g_2^{-1} * x) = (g_1 \cdot g_2^{-1}) * x$ (IV)

By (II), (III), and (IV), $x = (g_1 \cdot g_2^{-1}) * x$. Hence $g_1 \cdot g_2^{-1} \in G_x$. ■

Next we prove the orbit-stabilizer theorem which has many

Orbit-Stabilizer theorem

Tuesday, June 29, 2021 3:29 PM

implications.

<u>Theorem</u> (The Orbit-Stabilizer theorem) Suppose $G \curvearrowright_* X$.

Then, for every x, the following is a bijection:

$$f: G/G_x \longrightarrow G * x, \quad f(gG_x) := g * x.$$

In particular, $[G : G_x] = |G * x|$.

<u>Pf.</u> <u>Well-defined</u>. Since f is given in terms of a coset representative, we need to discuss why it is well-defined.

$$g_1 G_x = g_2 G_x \Rightarrow g_1^{-1} g_2 \in G_x \Rightarrow (g_1^{-1} g_2) * x = x$$

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

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

$$\Rightarrow g_2 * x = g_1 * x.$$

<u>injective</u>. $f(g_1 G_x) = f(g_2 G_x) \Rightarrow g_1 * x = g_2 * x$

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

$$\Rightarrow \underbrace{(g_1^{-1} g_1)}_{e_G} * x = (g_1^{-1} g_2) * x$$

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

$$\Rightarrow g_1^{-1} g_2 \in G_x \Rightarrow g_1 G_x = g_2 G_x.$$

Orbit-Stabilizer theorem

Tuesday, June 29, 2021 3:29 PM

<u>Surjective</u>. Every element of $G * x$ is of the form $g * x$, and so it can be written as $f(gG_x)$. Hence every element of the codomain of f is in its image. Therefore f is surjective. ∎

The orbit-stabilizer theorem has many implications. Here we focus on finite groups of order p^n where p is prime.

<u>Theorem</u> Suppose $(P, \cdot)$ is a group and $|P| = p^n$ where p is prime and $n \in \mathbb{Z}^+$. Suppose X is a finite set and $P \curvearrowright_* X$. Let X^P be the set of fixed points of P; that means

$$X^P := \{x \in X \mid \forall g \in P,\ g * x = x\}.$$

Then
$$|X| \equiv |X^P| \pmod p.$$

<u>Pf</u>. Since the set ${}_P\backslash X$ of all P-orbits is a partition of X, $|X| = \sum_{P*x \in {}_P\backslash X} |P*x|$. By the orbit-stabilizer theorem, $|P*x| = [P : P_x]$. We also notice that $x \in X^P$ if and only if $|P*x| = 1$ if and only if $P_x = P$. Hence we obtain

$$|X| = \sum_{P*x \in {}_P\backslash X,\ P_x \neq P} [P : P_x] + \underbrace{\sum_{P*x \in {}_P\backslash X,\ |P*x| = 1} 1}_{\to |X^P|}$$

Groups of prime order

Tuesday, June 29, 2021 3:29 PM

By Lagrange's theorem, $|P| = |P_x|\,[P:P_x]$. Hence $[P:P_x]$ divides $|P| = p^n$. Earlier we have proved that every divisor of p^n is either 1 or a multiple of p (in fact, using this result one can show that the set of positive divisors of p^n is $\{1, p, \ldots, p^n\}$.)

Hence if $P_x \neq P$, then $[P:P_x] \overset{p}{\equiv} 0$. Therefore

$$|X| = \sum_{\substack{P * x \in P\backslash X \\ P_x \neq P}} [P:P_x] + |X^P| \overset{p}{\equiv} |X^P|. \qquad \blacksquare$$

One of the implications of the above theorem is the following partial converse of Lagrange's theorem.

<u>Theorem (Cauchy)</u> Suppose G is a finite group and p is a prime factor of $|G|$. Then there is $g \in G$ which has order p.

We present a beautiful proof of this result. Here is a main idea: we want to find a non-trivial solution of $x^p = e_G$. Instead we look at a "more relaxed" equation which has "a lot of symmetries":

$x_0 x_1 x_2 \cdots x_{p-1} = e_G$, and view our desired equation $x^p = e_G$ as a "section" of this new equation: $x_0 = x_1 = \cdots = x_{p-1} = x$.

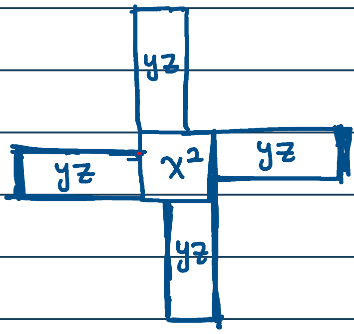
Cauchy's theorem

Tuesday, June 29, 2021 3:29 PM

This type of idea has been used in number theory for finding integer solutions for certain equations. I encourage you to search for Heath-Brown's proof of the following theorem of Fermat:

$$p: \text{prime and } p \overset{4}{\equiv} 1 \implies \exists x,y \in \mathbb{Z},\ p = x^2 + y^2.$$

There again the idea is to "relax" the equation and get "a lot of symmetries": $p = x^2 + 4yz$. Geometrically



Proof of Cauchy's theorem.

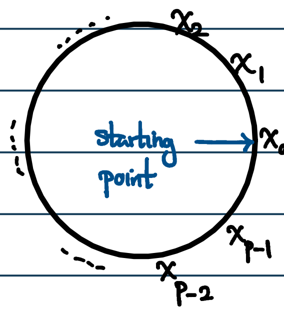
Let $X := \{(x_0, x_1, \ldots, x_{p-1}) \in G \times \cdots \times G \mid x_0 x_1 \cdots x_{p-1} = e_G\}$.

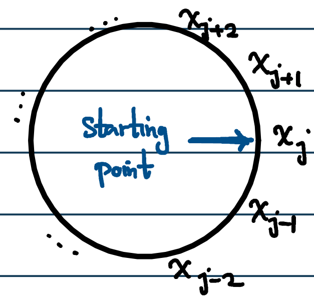
- Notice that $(x_0, x_1, \ldots, x_{p-1}) \in X \iff x_{p-1} = (x_0 x_1 \cdots x_{p-2})^{-1}$, and so $X = \{(x_0, x_1, \ldots, x_{p-2}, (x_0 \cdots x_{p-2})^{-1}) \mid x_0, x_1, \ldots, x_{p-2} \in G\}$. This implies that $|X| = |G|^{p-1}$.
- Next we observe that

$$x_0 x_1 \cdots x_{p-1} = e_G \implies x_0 x_1 \cdots x_{j-1} = (x_j \cdots x_{p-1})^{-1}$$
$$\implies x_j x_{j+1} \cdots x_{p-1} x_0 x_1 \cdots x_{j-1} = e_G,$$

and so $(x_0, x_1, \ldots, x_{p-1}) \in X$ implies that $(x_j, \ldots, x_{p-1}, x_0, \ldots, x_{j-1}) \in X$.

Hence we can cyclically move the coordinates and get a possibly different point of X. This gives us an action of $\mathbb{Z}_p$ on X:





$$[j]_p * (x_0, x_1, \dots, x_{p-1}) := (x_j, \dots, x_{p-1}, x_0, \dots, x_{j+1}).$$

Notice that $[j]_p * \cdots$ simply adds $[j]_p$ to the index, and so $[i]_p * ([j]_p * \cdots)$ adds $([i]_p + [j]_p)$ to the index, which means that it is the same as $([i]_p + [j]_p) * \cdots$. Hence $*$ gives us an action of $\mathbb{Z}_p$ on X. Since $|\mathbb{Z}_p| = p$ is prime,

(I) $|X| \equiv |X^{\mathbb{Z}_p}| \pmod p$. Because $|X| = |G|^{p-1}$ and $p \mid |G|$,

(II) $|X| \overset{p}{\equiv} 0$. Hence $p \mid |X^{\mathbb{Z}_p}|$. Notice that

$$(x_0, x_1, \dots, x_{p-1}) \in X^{\mathbb{Z}_p} \iff \forall j,\ [j]_p * (x_0, \dots, x_{p-1}) = (x_0, \dots, x_{p-1})$$

$$\iff \forall j,\ (x_j, \dots, x_{p-1}, x_0, \dots, x_{j-1}) = (x_0, \dots, x_{p-1})$$

$$\iff x_0 = x_1 = \cdots = x_{p-1}.$$

Therefore $X^{\mathbb{Z}_p} = \{(x, x, \dots, x) \in G \times \cdots \times G \mid x^p = e_G\}$. Notice that $(e_G, \dots, e_G) \in X^{\mathbb{Z}_p}$, and so $|X^{\mathbb{Z}_p}| \geq 1$ and $p \mid |X^{\mathbb{Z}_p}|$ by (I) and (II)

Sylow's first theorem

Tuesday, June 29, 2021 3:29 PM

$\Rightarrow |X^{\mathbb{Z}_p}| \geq p \Rightarrow \exists (x, \ldots, x) \in X$ which is not $(e_G, \ldots, e_G)$.

$\Rightarrow \exists\, x \neq e_G$ and $x^p = e_G$.

$\Rightarrow o(x) \neq 1$ and $o(x) \mid p$

$\Rightarrow o(x) = p$ as p is prime. ∎

Next we inductively prove the following result of Sylow:

<u>Theorem</u> (Sylow's 1st theorem) Suppose G is a finite group and $p^k \mid |G|$ where p is prime and k is a positive integer. Then there is a chain of subgroups $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_k$ of G such that $|P_i| = p^i$.

<u>Pf.</u> We proceed by induction on k. Base of induction ($k=1$) follows from Cauchy's theorem. So we focus on the induction step. Suppose $p^{k+1} \mid |G|$. Then $p^k \mid |G|$, and so by the induction hypothesis, there is a chain of subgroups $P_1 \subseteq \cdots \subseteq P_k$ such that $|P_i| = p^i$. Let $P_k \curvearrowright G/P_k$ by the left multiplication: $x \cdot (gP_k) := xg\, P_k$. Since $|P_k| = p^k$, $|G/P_k| \equiv |(G/P_k)^{P_k}|$ (mod p). Notice that $|G/P_k| = \frac{|G|}{p^k}$.

Sylow's first theorem

Tuesday, June 29, 2021 3:29 PM

Since $p^{k+1} \mid |G|$, $p \mid \frac{|G|}{p^k}$. Hence $p \mid |G/P_k|$. Therefore

$p \mid |(G/P_k)^{P_k}|$. Next we describe elemen

Final remarks

Tuesday, June 29, 2021 3:29 PM

of subgroups of prime power order of a finite group, and their proofs are based on $|X| \equiv |X^P| \pmod{p}$ for a right choice of X and P.

I hope that you enjoyed group theory, and next time that you face a new problem you start asking yourself whether you can use symmetries to attack it!