CCS Discrete Math I | Professor: Padraic Bartlett

Homework 11: Group Actions

Due Friday, Week 6 | *UCSB 2014*

Do **three** of the **six** problems below!

These problems are all centered on the idea of a **group action**. This is an incredibly valuable concept that we didn't have time to cover in class but I want you to see a bit of; hence this problem set! We define the relevant terms here:

Definition. A **group action** of a group $\langle G, \cdot \rangle$ on a set X is any map $\star : G \times X \to X$ that satisfies the following two properties:

1. **Identity**: If e is the identity in G, then for any $x \in X$, we have $e \star x = x$.
2. **Compatible with the group operation**: For any two elements $g, h \in G$ and any element $x \in X$, we have $g \star (h \star x) = (g \cdot h) \star x$.

The idea with this second operation is that it says that it doesn't matter whether we apply g, h one-by-one using $\star$ to x, or if we combine them first in G with $\cdot$ and then apply the result to x. In both cases we get the same thing!

Example. Take the group S_n, and consider the following action of this group on the set $\{1, 2, \dots n\}$: for any $\sigma \in S_n, k \in \{1, \dots n\}$, set $\sigma \star k = \sigma(k)$. For example, if $\sigma = (123)$ and $k = 2$, we would say $\sigma(2) = 3$.

This is a group action! To see this, we just check our definition:

1. **Identity**: The identity of S_n is just the identity map id on $\{1, \dots n\}$. Therefore, for any $k \in \{1, \dots n\}$ we have $id \star k = id(k) = k$: so we satisfy the identity property!
2. **Compatible with the group operation**: Take any two permutations $\sigma, \varphi \in S_n$, and any $k \in \{1, \dots n\}$. Notice that $(\sigma \circ \varphi) \star (k) = \sigma(\varphi(k))$, and $\sigma \star (\varphi \star k) = \sigma \star (\varphi(k)) = \sigma(\varphi(k))$ is just the same thing; therefore we are compatible with our group's operation!

Given a group operation, a useful pair of concepts to consider are the ideas of **orbit** and **stabilizers**:

Definition. Given any group $\langle G, \cdot \rangle$ acting on a set X by some operation $\star$, take any $x \in X$. The **orbit** of x is the subset of X given by

$$G \star x := \{y \in X \mid \exists g \in G, g \star x = y\}$$

This, in a sense, is the collection of all possible elements in X that x can be "taken to" by $\star$.

Similarly, the **stabilizer** of G is the subset of G given by

$$G_x := \{g \in G \mid g \star x = x\}.$$

This is the collection of all possible group elements in G that "fix" x.

When doing problems below, you can use any of the other problems on this set, even if you didn't successfully prove that other problem.

1. (a) Take the group D_{2n}, and consider the following way in which it could act on the set of vertices $\{v_1, \ldots v_n\}$ of a n-gon: if f is a symmetry of our n-gon, then we say that $f \star v_k$ is just $f(v_k)$. In other words, our action sends v_k to whatever vertex f maps v_k to. Show that this is a group action of D_{2n} on $\{v_1, \ldots v_n\}$

   (b) For any group $\langle G, \cdot \rangle$, consider the following way in which G could "act" on itself: for any $g \in G, h \in G$, set $g \star h = g \cdot h$. Show that this is a group action of G on G.

2. Take any group $\langle G, \cdot \rangle$ acting on a set X. Take any $x \in X$. Show that the stabilizer of x, as defined above, is a subgroup of G.

3. Take any group $\langle G, \cdot \rangle$ acting on a set X. Fix any element $x \in X$, and look at the orbit of x. Show that the number of elements in the orbit of x is just $|G|/|G_x|$, where G_x is the stabilizer of x, as defined earlier. (Hint: look at cosets of G_x!)

4. In class, we proved Fermat's little theorem. In this problem, we provide an alternate proof!

   Take any prime p, and any $a \in \{1, \ldots p-1\}$. Take a necklace with p beads, and give each bead a color from a set of a different colors: $C = \{c_1, c_2, \ldots c_a\}$: this gives us a sequence

   $$(b_1, b_2, \ldots b_p)$$

   of colored beads, with each $b_i \in C$. Notice that there are a^p many such beads.

   (a) We can act on this set of necklaces by $\langle \mathbb{Z}/p\mathbb{Z}, + \rangle$ as follows: given a necklace $B = (b_1, \ldots b_p)$ and a value $k \in \mathbb{Z}/p\mathbb{Z}$, set $k \star B$ equal to the necklace given by shifting the beads in B k beads over to the right cyclically. In other words, set

   $$k \star (b_1, \ldots b_p) = (b_{k+1}, b_{k+2}, \ldots b_p, b_1, b_2, \ldots b_k).$$

   Prove that this is a group action.

   (b) Show that the total number of necklaces modulo p is a. Conclude that $a^p \equiv a \mod p$, which is Fermat's little theorem!

5. On HW #7, problem 1, we studied the Bell numbers, and proved the relation

   $$B_{n+2} \equiv B_n + B_{n+1} \mod 2.$$

   Generalize this result as follows:

   $$B_{n+p} \equiv B_n + B_{n+1} \mod p.$$

   (Hint: think about partitions of the set $\{1, 2, 3, \ldots n, a_1, a_2, \ldots a_p\}$. Act on any such partition π of this set by $\langle \mathbb{Z}/p\mathbb{Z}, + \rangle$, where for any $k \in \mathbb{Z}/p\mathbb{Z}$ we have $k \star \pi =$ the partition where we've replaced each a_m with $a_{(m+k) \mod p}$. What do the orbits look like? What can you conclude?)

6. Crack the encrypted text on the next page. It may be helpful to download the .tex file so you can extract the plaintext here.

Ciphertext

Bo. mca Ygp. Pjoeabk, dc zjjnto rdrd, Eoukbf Soukb, itoq eoaja fd pmn qtpq fwbk lbdt mqgcqrqxn kagjma, qtpkw nlg kbdn jgre. Fwbk lbdt qtt imhq btlbab kdr'p tubtzf il nt fzklxkbp xk mcvfwfzv pfgxzvb ag jkhqqgfajp, ntzmjpq ieqn gghq pxaz'i eaaa ixqt hrow kacpqcpq. Bo. Pjoeabk lxe ieq sfdtzfdo au x rxoy rxxabp Vogckucde, leure ypaq souaie. Wb ipp m qfs, qbquv ypk ixqt wxdsik pkk cboz, xxieajdt wb pxa tpsq p sqgv xpost jghqmreq. Boe. Srdhiqn tmh qtxk mca nalzsb mca tpa ztxdav flfot qtt rejxx pjajkf dc ztzw, leure opjq xk htok jpqurx pp ewb eebzi pa brow lr wbd ifyt zdpkucd akbd vxdsbz ubzrbe, hmkxks dk fwb ztfswyagp. Fwb Pjoeabkh ems x ebxxa pac zmaiqs Agsiqn xzs fz ieqxo aefzxlz ieqgb ipp zd cucbd qlk pkkleqgb. Fwb Pjoeabkh ems bhtokieucd fwbk lxzibp, qrf ieqn xxhl tpa m hbogbf, pkp ieqxo sgbmibei cqpo ipp fwxf hlytyasv idrxs auhzakbd xq. Fwbk sfpc'q fwfzz qttv odrxs yqpo ui fr pkkdkq ulgca ajq mqlgi qtt Maiqqgp. Ygp. Bdqfto ipp Ygp. Pjoeabk'h puhqqg, ygi qttv tpaz'i jqi cag pqkbdpi ktxdh; fz uxoi, Jdh. Aggpxtv bgbftkpta ewb pxaz'i emkb m hfeibd, qbopret eqg puhqqg xzs eqg dada-rdo-zdqtxks wreqxzs tqgb mh rzSrdhiqnfew xe xq ipp bdpexyxt qa qb. Fwb Pjoeabkh ptjaptoqs qa ieuch iwxf ieq cbuvendoe llgaa epv uu qtt Maiqqgp mgoukbp xk fwb eioqtq. Fwb Pjoeabkh hztt fwxf ieq Elfibdh ems x ebxxa pac, qad, ygi qttv tpa ztsqg bhtk etbz wfy. Ieuh yan tmh xzdqtto sdlp gbmhlz uld zbqefzv qtt Maiqqgp mlxk; ieqn ausk'f lxzi Agsiqn jumfzv tuie m reuaa xxhq iemi. Tttk Yg. xzs Jdh. Aggpxtv idhq jm ac qtt agai, sgxk Irqhamn lgg pfdok hqmgqe, ieqgb ipp zdqtxks pyajq fwb oalgsv ezv ajqexaq il ejdstpf iemi pfgxzvb mca ynpftoudre ieucde llgaa edlz qb tpmbtkucd mai akbd ieq rlgcqdn. Jd. Srdhiqn egbjqs xe wb bxzwta ajq txp ydpf qldxks ifq uld lldz, xzs Jdh. Aggpxtv sdpexmqs xipv tpmbxik pp ewb igbeiiqs x eroqpjucd Pjaxtv ucqa wfe wfsw ztpfd. Clzt lr ieqb kaifota m axdvb, fptzn lia cxjqfto bppf ieq lfzsli.