GROUPS AND BURNSIDE'S LEMMA PROBLEMS

AKASH DHIRAJ

$(*)$ = hard; $(\dagger)$ = important.

Advice. If you think you have the solution to a problem, you don't need to attempt it.

Remark. Some of these problems are my own creation. This being the case, it's possible for there to be errors in some of them. Please bring flawed problems to my attention.

1. Introductory Group Theory

(1) Check that $\mathbb{Z}/n\mathbb{Z}$ is indeed a group. $(\dagger)$
   (a) Show that if $a+n\mathbb{Z} = a'+n\mathbb{Z}$ and $b+n\mathbb{Z} = b'+n\mathbb{Z}$, then $(a+b)+n\mathbb{Z} = (a'+b')+n\mathbb{Z}$. This shows that our operation is well-defined.
   (b) Now, show that the group satisfies the group axioms. I.e. state what the identity element is, what inverses of $a+n\mathbb{Z}$ are, and why the group operation is associative (feel free to assume standard addition in $\mathbb{Z}$ is associative).

(2) Check that S_n is a group. When we did this in our lecture, our proof of the existence of inverses was a bit sketchy. Make this part of the proof more rigorous by explaining why "g is well-defined and bijective from the bijectivity of f."

(3) Preceding our definition of a subgroup, we said

> "The most natural way to define 'subgroup' is a subset who is a group with the same operation."

Why does the definition we provided do this? More specifically, we ask why closure under the group operation and the existence of inverses imply that our subset contains an identity element? (associativity is trivial) $(\dagger)$

(4) Consider a regular n-gon with side length 1 and a single vertex centered at the point $(0, 1)$ in the cartesian plane. The group D_n consists of the symmetries of this regular n-gon. I.e. the rigid motions from $\mathbb{R}^2 \to \mathbb{R}^2$ that permute the vertices of the regular n-gon amongst themselves. Seeing as our group consists of functions, the natural group operation is function composition. $(*)$
   (a) How many elements does D_n have?
   (b) Do your best to describe this group. What do inverses look like? What does the identity look like?
   (c) $g_1, \dots, g_n$ are the generators of a group G if every element is a product of powers $g_1, \dots, g_n$. So, for example, the generator of $\mathbb{Z}$ is 1. Can you say what the generators of D_n are? What is the smallest number of generators? $(*)$

(5) Show that the set of nth roots of unity form a group under multiplication. Skip this if you don't know complex numbers. Otherwise, $(\dagger)$.

(6) Look for a convenient way to evaluate the order of an element in S_n. $(*, \dagger)$

(7) Show that if every element is equal to it's inverse, then the group is abelian. $(\dagger)$

(8) We saw that $\mathbb{Z}$ doesn't form a group under multiplication. But, $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ does for prime p. Why? Remember Bezout's Lemma! $(*)$

2. Group Actions & Burnside's Lemma

(1) Let a finite group G act on a finite set X. We say our group action is transitive if there is only one orbit in X. I.e. for all $x, y \in X$, there exists $g \in G$ such that $gx = y$. Now, for such a group action, suppose that $gx \neq x$ for all $g \in G \setminus \{e\}$. Prove that $|G| = |X|$.

(2) Show that the 15 puzzle is not solvable. $(***)$[1] (†)

(3) With our knowledge of Lagrange's Theorem, we'll explore Euler's totient theorem. (†)

(a) As you might guess, the standard group of integers of modulo n doesn't form a group under multiplication because we lack inverses. A natural question to ask is what the biggest subset of integers modulo n that form a group under multiplication are. Show that this set consists of elements of the form $a + n\mathbb{Z}$ for a such that $\gcd(a, n) = 1$. Remember Bezout's Lemma!

(b) $\phi(n)$ denotes the number of positive integers m less than n such that $\gcd(m, n) = 1$. With this in mind, prove Euler's theorem:

Theorem 2.1 (Euler)**.** *For a positive integer n and integer a relatively prime to n,*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

(4) Prove Cayley's Theorem: $(*, \dagger)$

Theorem 2.2 (Cayley)**.** *Let $|G|$ be finite. Then, G is isomorphic to some subgroup of the symmetric group S_n.*

(5) Let p be a prime and the Fibonacci numbers be the elements of the sequence $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$. Prove $p \mid F_{2p(p^2-1)}$. $(*)$

3. Using Burnside's Lemma

(1) Prove Proposition 17. (∗,†) That is, prove that there are

(a) $3(2n^3 + n^4)$ cubes fixed by rotations about an axis passing through the centres of opposite faces.

(b) $8n^2$ cubes fixed by rotations about an axis passing through two vertices.

(c) $6n^3$ cubes fixed by rotations about an axis passing through the mid-points of edges.

(d) n^6 cubes fixed by the identity rotation.

(2) Use Burnside's Lemma to count the number of ways to color the edges of a hexagon each either red or blue, where two colorings are considered the same if one is a rotation of the other. (†)

(3) Two of the squares of a 7×7 checkerboard are painted yellow, and the rest are painted green. Two color schemes are equivalent if one can be obtained from the other by applying a rotation in the plane of the board. How many inequivalent color schemes are possible? **[AIME 1996]**

(4) Taotao wants to buy a bracelet consisting of seven beads, each of which is orange, white or black. (The bracelet can be rotated and reflected in space.) Find the number of possible bracelets. **[PUMaC 2009]**

[1] This is particularly hard because you don't know many facts about the symmetric group yet. Still, I want you to think about this problem! It might be a mini-lesson if we continue talking about groups

4. Hints to Selected Problems

(1.4) Cut out a piece of paper in the shape of a regular n-gon and try to figure out the number of symmetries. Then, see if you can write every symmetry in terms of a single reflection and a rotation by $2\pi/n$.

(1.6) Consider a single cycle $(a_1, \dots, a_n) \in S_n$. What is $(a_1, \dots, a_n)^n$? What is $(a_1, \dots, a_n)^m$ for $m < n$?

(1.8) In case you're a little rusty on number theory,

Theorem 4.1 (Bezout). *For integers $a, b \in \mathbb{Z}$ with $\gcd(a, b) = d$, there exists $s, t \in \mathbb{Z}$ such that*

$$as + bt = d.$$

The proof is essentially the Euclidean Algorithm.

(2.4) Pick $g \in G$. Left multiplication of g on G induces a permutation of the set G. Use this to set up your map $f : G \to S_{|G|}$. Prove f is an injective homomorphism.

(2.5) Consider the group

$$G := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}/p\mathbb{Z}, ad - bc \equiv \pm 1 \pmod{p} \right\}.$$

Find $|G|$ and use that

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

to conclude the desired result.

Email address: akashdhiraj2019@gmail.com

Math Circle