Team Round

Lexington High School

April 7, 2018

Potpourri [70]

1. Points $P_1, P_2, P_3, \cdots, P_n$ lie on a plane such that $P_aP_b = 1, P_cP_d = 2$, and $P_eP_f = 2018$ for not necessarily distinct indices $a, b, c, d, e, f \in \{1, 2, \cdots, n\}$. Find the minimum possible value of n.

2. Find the coefficient of the x^2y^4 term in the expansion of $(3x+2y)^6$.

3. Find the number of positive integers $n < 1000$ such that n is a multiple of 27 and the digit sum of n is a multiple of 11.

4. How many times do the minute hand and hour hand of a 12-hour analog clock overlap in a 366-day leap year?

5. Find the number of ordered triples of integers (a, b, c) such that $(a+b)(b+c)(c+a) = 2018$.

6. Let S denote the set of the first 2018 positive integers. Call the *score* of a subset the sum of its maximal element and its minimal element. Find the sum of score(x) over all subsets $s \in S$

7. How many ordered pairs of integers (a, b) exist such that $1 \le a, b \le 20$ and a^a divides b^b?

8. Let f be a function such that for every non-negative integer p, $f(p)$ equals the number of ordered pairs of positive integers (a, n) such that $a^n = a^p \cdot n$. Find

$$\sum_{p=0}^{2018} f(p).$$

9. A point P is randomly chosen inside a regular octagon $A_1A_2A_3A_4A_5A_6A_7A_8$. What is the probability that the projections of P onto the lines $\overleftrightarrow{A_iA_{i+1}}$ for $i = 1, 2, \cdots, 8$ lie on the segments $\overline{A_iA_{i+1}}$ for $i = 1, 2, \cdots, 8$ (where indices are taken mod 8)?

10. A person keeps flipping an unfair coin until it flips 3 tails in a row. The probability of it landing on heads is $\frac{2}{3}$ and the probability it lands on tails is $\frac{1}{3}$. What is the expected value of the number of the times the coin flips?

Long Answer [130]

Group theory is a rich and diverse theory of mathematics that is the fundamental building block of many other branches of math such as abstract algebra. It has countless applications in physics or in the real world as well: for example, the symmetries of a space can be modelled using group theory, and the Rubik's cube can easily be modelled (and solved) in terms of group theory. This set of problems will introduce groups and will prove a fact about certain sub-types of groups.

A group G is a **set** of elements closed under an **operation** $\cdot$ such that the following hold for all $a, b, c \in G$:

1. The operation is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$
2. G contains an identity: an element e, such that $a \cdot e = e \cdot a = a$ for all $a \in G$
3. Every element a has an inverse: that is, an element $b = a^{-1}$ in G such that $a \cdot b = b \cdot a = e$.

For example, the integers $\mathbb{Z}$ under the operation + forms a group. The identity is $e = 0$. The inverse of a is $-a$. Clearly addition is associative in the integers.

1. **[2]** Consider the integers $\mathbb{Z}$ under multiplication $\times$. Does this form a group? Why or why not?

Starting from now, we will omit the $\cdot$ between elements, and refer to expressions such as $a \cdot b$ simply as ab.

2. **[6]** Show that in a group, there can only be one identity. That is, if e and e' are two identities, then $e = e'$.

One should be careful to note that the operation of a group is not always commutative. That is, we will not always have $ab = ba$.

3. **[3]** Let $x, y, z, w \in G$ where the operation of G is not commutative. Express y in terms of x, z, w and their inverses, given that $xyz^{-1}w = e$. Be careful with how you multiply!

We say a group is *cyclic* if there exists an element $g \in G$ such that every element $a \in G$ is equal to $g^k = \underbrace{g \cdot g \cdots \cdot g}_{\text{k times}}$ for some integer k. That is, $G = \{g^k : k \in \mathbb{Z}\}$. We say G is *generated* by g.

The integers $\mathbb{Z}$ under addition form a cyclic group, as one can express every integer as some (possibly negative) amount of applications of addition to the element 1.

4. **[4]** Consider the group with elements 1,2,3,4 with operation as integer multiplication modulo 5. For example, we have $2 \cdot 3 = 1$. Show that this group is cyclic.

A subset H of a group G is a *subgroup* if it satisfies the following properties (using the same operation descended from G):

1. If a, b are in H, then ab is in H.
2. The identity e in G is also in H.
3. If a is in H, then it has an inverse a^{-1} in H that is the same as defined above.

For example, the set $H = 2\mathbb{Z}$, all even integers, forms a subgroup of $G = \mathbb{Z}$, the integers with the operation of addition.

From here on out, we will only consider groups with finitely many elements. The case of infinite groups has a similar theory but is slightly more complicated. We introduce our first theorem: We will prove that every subgroup H of a cyclic group G is cyclic.

Suppose G is generated by g. To begin, we define the integer n to be the smallest positive integer such that g^n is in H.

5. **[9]** Consider an arbitrary element h in H. Show that h is an integer power of g^n. *Hint:* Let $h = g^a$.
6. **[1]** Conclude that H is cyclic.

We define the *order* of an element $x \in G$ to be the smallest positive integer n such that $x^n = e$.

For example, consider the complex numbers without 0, written $\mathbb{C}^\times$, as a group under the operation of multiplication. Then i has order 4, as $i^4 = 1$.

7. **[5]** Let G be a finite group. Show that the order of every element is finite.
8. **[7]** Let $x \in G$ have order n. Show that $x^k = e$ if and only if k is divisible by n.

Let $x \in G$ have order n and let k be an arbitrary positive integer. The following problems will demonstrate the following theorem: The order of x^k is $n/\gcd(k,n)$.

9. **[4]** Let t be the order of x^k. Show that $kt = nm$ for some integer m.
10. **[9]** Define n' and k' to be integers such that $n = \gcd(n,k)n'$ and $k = \gcd(n,k)k'$. Show that $n' \leq t$.
11. **[8]** Show that $(x^k)^{n'} = e$ and conclude that $t \leq n'$. Finish the proof of the theorem.

We now return our attention to cyclic groups.

12. **[11]** Show that the size (number of elements) of each subgroup H of a cyclic group G divides the size of G.
13. **[3]** Let $|G|$ denote the size (number of elements) of the group G. Show that for any element $g \in G$, it is true that $g^{|G|} = e$.
14. **[6]** Let d divide the size of a cyclic group G. Show that there exists a subgroup H of G that has size d.

We conclude our classification with the following theorem: Let G have size m, and let g generate G. Then the subgroup generated by g^k is the same as the subgroup generated by $g^{\gcd(m,k)}$.

To prove this, we will show that g^k is a power of $g^{\gcd(m,k)}$ and that $g^{\gcd(m,k)}$ is a power of g^k.

15. **[2]** Show that g^k is a power of $g^{\gcd(m,k)}$.
16. **[14]** Bezout's identity states that
$$\gcd(k,m) = kx + my$$
for some integers x, y. Finish proving the theorem. *Hint:* Use this to express $g^{\gcd(k,m)}$ as a power of g^k.
17. **[4]** Show that there cannot exist two distinct subgroups H_1, H_2 of G with equal sizes.

When considering objects in algebra, it is often equally important—if not more important—to consider relationships between those objects. Thus we introduce the concept of **group homomorphisms**:

Let G, H be groups. A map (function) $\phi : G \to G'$ is a **homomorphism** if it preserves the operation. That is, for all elements $g_1, g_2 \in G$ we have
$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2).$$
This is a little tricky; note that the $\cdot$ in the left-hand side is the operation in G while the $\cdot$ in the right-hand side is the operation in G'.

For the following problems we consider a homorphism $\phi : G \to G'$.

18. **[2]** Let e_G be the identity in G and $e_{G'}$ be the identity in G'. Show that $\phi(e_G) = e_{G'}$.
19. **[2]** Show that for $g \in G$, we have $\phi(g^{-1}) = \phi(g)^{-1}$.

The **kernel** of ϕ is defined to be
$$\ker(\phi) = \{g \in G | \phi(g) = e\}$$
.

20. **[4]** Show that $\ker(\phi)$ forms a subgroup of G.

The **image** of ϕ is defined to be

$$\mathrm{im}(\phi) = \{\phi(g) | g \in G\}$$

.

21. **[4]** Show that $\mathrm{im}(\phi)$ forms a subgroup of G'.

Let H be a subgroup of G. Define the sets (subgroups)

$$gH = \{g \cdot h | h \in H\}$$

and

$$Hg = \{h \cdot g | h \in H\}.$$

These subgroups are called *left and right cosets of* H, respectively. H is called **normal** if $gH = Hg$ for all $g \in G$.

The concept of normal subgroups is necessary for defining quotients (but perhaps is not obvious why):

Let H be a normal subgroup of G. The set of right cosets (an equivalent definition can be made with left cosets) of H then forms a group, under the following operation:

$$(g_1 H) \cdot (g_2 H) = (g_1 \cdot g_2) H.$$

This group is denoted G/H.

It is true that for $\phi : G \to G'$, $\ker(\phi)$ and $\mathrm{im}(\phi)$ are normal subgroups of their respective groups. Now let $\phi : G \to G'$ be a homomorphism.

A map $\phi : G \to G'$ is an **isomorphism** if it is bijective. We say G, G' are isomorphic and denote this as $G \simeq G'$.

This final result is know as the first isomorphism theorem for groups.

22. **[20]** Show that $\mathrm{im}(\phi) \simeq G/\ker(\phi)$.