UT Putnam Prep 2018-11-15 — Group Theory

This is a comparatively advanced topic but still becomes fodder for some Putnam questions. I don't want to exclude students who have not take M343K/M373K so let me give the briefest possible introduction to the topic.

In high school you learn about logarithms. The upshot is that they enable you to mirror multiplication (of positive numbers) by means of addition. That is, both operations have the following structure:

1. You have a set of things that you combine with an operation "*"
2. The associative law holds for this operation
3. There is a "neutral thing" e which makes $a * e = e * a = a$ for every a.
4. Every element a has its opposite, b, for which $a * b = b * a = e$.

The two examples at hand are the set of all real numbers, where "*" means addition (and so $e = 0$), and the set of positive real numbers, where "*" is multiplication (in which case $e = 1$). But there are many other examples of such systems; any such an example is called a *group*. Some famous examples:

A. The set of all 2×2 invertible matrices, with "*" being matrix multiplication

B. The set consisting only of symbols 0 and 1, the operation being addition-modulo-2

C. Any vector space you have ever met, the operation being addition of vectors

D. The set of all permutations of a set S, that is, functions $f : S \to S$ which are one-to-one and onto; the operation "*" means composition (i.e. "first do the one on the right, then do the one on the left")

E. The set of ways of scrambling the 54 tiles on the Rubik's Cube. (Again "*" means composition).

Notice that I haven't mentioned the commmutative law. Some examples have it, some don't. When a group's operation satisfies the commutative property we say the group is *abelian*. (This is, by the way, the only example I know where we don't capitalize the name of the mathematician being commemorated!)

I also didn't mention the distributive law because that property makes mention of there being *two* operations at once. Structures that have two operations are called *rings* if they meet some mild conditions (like the distributive law), and the study of them is a whole separate chapter in Abstract Algebra. A setting in which you can add, subtract, multiply,*and* divide is called a *field* and, all things considered, these are a lot less exotic than groups and rings but very useful and interesting too!

There are many, many theorems that apply to all groups, many of them quite trivial but important (for example, axiom 3 doesn't say there can't be more than one such e but that's a theorem anyway). Of the nontrivial theorems I think I would primarily stress *Lagrange's Theorem:* if G is a finite group, and H is a subgroup of G (i.e. it's a subset of G closed under the group operation) then the number of elements of H divides the number of elements of G. I leave it to the class to discuss other useful theorems.

Let's try some questions.

1. In the additive group of ordered pairs of integers (m, n) (with addition defined componentwise), consider the subgroup H generated by the three elements

$$(3, 8) \qquad (4, 1) \qquad (5, 4).$$

Then H has another set of generators of the form

$$(1, b) \qquad (0, a)$$

for some integers a, b with $a > 0$. Find a. [Putnam 1975-B1]

2. Let r, s, t be positive integers that are relatively prime in pairs. Let G be an abelian group and a, b be elements of G. Suppose $a^r = b^s = (ab)^t = e$ (the identity element of G). Show that $a = b = e$.

3. Show that a finite group can not be the union of two of its proper subgroups. Does the statement remain true if "two is replaced by "three? [Putnam 1969-B2]

4. Let H be a group generated by two elements $x, y \in H$ which satisfy $x^5y^3 = x^8y^5 = e$. Prove that $x = y = e$.

5. Let S be a non-empty set with an associative operation that is left and right cancellative ($xy = xz$ implies $y = z$, and $yx = zx$ implies $y = z$). Assume that for every a in S the set $\{a_n : n = 1, 2, 3, \ldots\}$ is finite. Must S be a group? [Putnam 1989-B2]

6. Let S be a set of real numbers which is closed under multiplication (that is, if a and b are in S, then so is ab). Let T and U be disjoint subsets of S whose union is S. Given that the product of any three (not necessarily distinct) elements of T is in T and that the product of any three elements of U is in U, show that at least one of the two subsets T, U is closed under multiplication. [Putnam 1995-A1]

7. Consider a set S and a binary operation * on S (that is, for each $a, b \in S$, $a * b$ is also in S). Assume that $(a * b) * a = b$ for all $a, b \in S$. Prove that $a * (b * a) = b$ for all $a, b \in S$. [Putnam 2001-A1]

8. Let x and y be elements in a ring-with-identity ("1"). Prove that if $1 - xy$ is invertible then so is $1 - yx$.

9. Suppose R is a ring in which for every element $a \in R$ we have $a^2 = a$. Show that R is commutative.

10. Show that if p is prime then $p | F_{2p(p^2-1)}$, where F_k is the kth Fibonacci number. ($F_1 = F_2 = 1$)

11. Suppose S is the collection of all subsets of a finite set X. For any $A, B \in S$ we write $A\Delta B$ for the *symmetric difference* of A and B, that is, the set of elements of X which lie in precisely one of A and B (not both). Show that for every $A, B, C, D \in S$

$$A\Delta B = C\Delta D \qquad \Longleftrightarrow \qquad A\Delta C = B\Delta D$$