

PUTNAM PROBLEMS

GROUP THEORY, FIELDS AND AXIOMATICS

The following concepts should be reviewed: group, order of groups and elements, cyclic group, conjugate elements, commute, homomorphism, isomorphism, subgroup, factor group, right and left cosets.

Lagrange's Theorem: The order of a finite group is exactly divisible by the order of any subgroup and by the order of any element of the group.

A group of prime order is necessarily commutative and has no proper subgroups.

A subset S of a group G is a set of *generators* for G iff every element of G can be written as a product of elements in S and their inverses. A *relation* is an equation satisfied by one or more elements of the group. Many Putnam problems are based on the possibility that some relations along with the axioms will imply other relations.

2001-A-1. Consider a set S and a binary operation $*$ on S (that is, for each a, b in S , $a * b$ is 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 .

1997-A-4. Let G be a group with identity e and $\phi : G \rightarrow G$ a function such that

$$\phi(g_1)\phi(g_2)\phi(g_3) = \phi(h_1)\phi(h_2)\phi(h_3)$$

whenever $g_1g_2g_3 = e = h_1h_2h_3$. Prove that there exists an element a in G such that $\psi(x) = a\phi(x)$ is a homomorphism (that is, $\psi(xy) = \psi(x)\psi(y)$ for all x and y in G).

1996-A-4. Let S be a set of ordered triples (a, b, c) of distinct elements of a finite set A . Suppose that:

1. $(a, b, c) \in S$ if and only if $(b, c, a) \in S$,
2. $(a, b, c) \in S$ if and only if $(c, b, a) \notin S$,
3. (a, b, c) and (c, d, a) are both in S if and only if (b, c, d) and (d, a, b) are both in S .

Prove that there exists a one-to-one function $g : A \rightarrow \mathbf{R}$ such that $g(a) < g(b) < g(c)$ implies $(a, b, c) \in S$. [Note: \mathbf{R} is the set of real numbers.]

1989-B-2. 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 $\{a^n : n = 1, 2, 3, \dots\}$ is finite. Must S be a group?

1987-B-6. Let F be the field of p^2 elements where p is an odd prime. Suppose S is a set of $(p^2 - 1)/2$ distinct nonzero elements of F with the property that for each $\alpha \neq 0$ in F , exactly one of α and $-\alpha$ is in S . Let N be the number of elements in the intersection $S \cap \{2\alpha : \alpha \in S\}$. Prove that N is even.

1979-B-3. Let F be a finite field having an odd number m of elements. Let $p(x)$ be an irreducible (*i.e.*, nonfactorable) polynomial over F of the form

$$x^2 + bx + c \quad b, c \in F .$$

For how many elements k in F is $p(x) + k$ irreducible over F ?

1978-A-4. A “bypass” operation on a set S is a mapping from $S \times S$ to S with the property

$$B(B(w, x), B(y, z)) = B(w, z)$$

for all w, x, y, z in S .

- (a) Prove that $B(a, b) = c$ implies $B(c, c) = c$ when B is a bypass.
- (b) Prove that $B(a, b) = c$ implies $B(a, x) = B(c, x)$ for all x in S when B is a bypass.
- (c) Construct a table for a bypass operation B on a finite set S with the following three properties: (i) $B(x, x) = x$ for all x in S . (ii) There exists d and e in S with $B(d, e) = d \neq e$. (iii) There exists f and g in S with $B(f, g) \neq f$.

1977-B-6. Let H be a subgroup with h elements in a group G . Suppose that G has an element a such that, for all x in H , $(xa)^3 = 1$, the identity. In G , let P be the subset of all products $x_1 a x_2 a \cdots x_n a$, with n a positive integer and the x_i in H .

- (a) Show that P is a finite set.
- (b) Show that, in fact, P has no more than $3h^2$ elements.

1976-B-2. Suppose that G is a group generated by elements A and B , that is, every element of G can be written as a finite “word” $A^{n_1} B^{n_2} A^{n_3} \cdots B^{n_k}$, where n_1, n_2, \dots, n_k are any integers, and $A^0 = B^0 = 1$, as usual. Also, suppose that

$$A^4 = B^7 = ABA^{-1}B = 1, \quad A^2 \neq 1, \quad \text{and} \quad B \neq 1.$$

- (a) How many elements of G are of the form C^2 with C in G ?
- (b) Write each such square as a word in A and B .

1975-B-1. In the additive group of ordered pairs of integers (m, n) (with addition defined component-wise), consider the subgroup H generated by the three elements

$$(3, 8) \quad (4, -1) \quad (5, 4) \quad .$$

Then H has another set of generators of the form

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

for some integers a, b with $a > 0$. Find a .

1972-B-3. Let A and B be two elements in a group such that $ABA = BA^2B$, $A^3 = 1$ and $B^{2n-1} = 1$ for some positive integer n . Prove $B = 1$.

1969-B-2. 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”?

1968-B-2. A is a subset of a finite group G , and A contains more than one half of the elements of G . Prove that each element of G is the product of two elements of A .