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.

2016-A-5. Suppose that G is a finite group generated by the two elements g and h, where the order of g is odd. Show that every element of G can be written in the form

$$g^{m_1}h^{n_1}g^{m_2}h^{n_2}\cdots g^{m_r}h^{n_r}$$

with $1 \le r \le |G|$ and $m_1, n_1, m_2, n_2, \ldots, m_r, n_r \in \{-1, 1\}$. (Here $|G|$ is the number of elements of G.)

2012-A-2. Let $*$ be a commutative and associative binary operation on a set S. Assume that for every x and y in S, there exists z in S such that $x * z = y$. (This z may depend on x and y.) Show that if a, b, c are in S and $a * c = b * c$, then $a = b$.

2012-A-5. Let $\mathbf{F}_p$ denote the field of integers modulo a prime p, and let n be a positive integer. Let v be a field vector in $\mathbf{F}_p^n$ and let M be an $n \times n$ matrix with entries in $\mathbf{F}_p$, and define $G : \mathbf{F}_p^n \to \mathbf{F}_p^n$ by $G(x) = v + Mx$. Let $G^{(k)}$ denote the $k-$fold composition of G with itself, that is $G * (1)(x) = G(x)$ and $G^{(k+1)}(x) = G(G^{(k)}(x))$. Determine all pairs p, n for which there exist v and M such that the p^n vectors $G^{(k)}(0)$, $k = 1, 2, \cdots, p^n$ are distinct.

2012-B-6. Let p be an odd prime such that $p \equiv 2 \pmod 3$. Define a permutation π of the residue classes modulo p by $\pi(x) \equiv x^3 \pmod p$. Show that π is an even permutation if and only if $p \equiv 3 \pmod 4$.

2011-A-6. Let G be an abelian group with n elements, and let

$$\{g_1 = e, g_2, \cdots, g_k\} \subseteq G$$

be a (not necessarily minimal) set of distinct generators of G. A special die, which randomly selects one of the elements $g_1, g_2, \cdots, g_k$ with equal probability, is rolled m times and the selected elements are multiplied to produce an element $g \in G$.

Prove that there exists a real number $b \in (0, 1)$ such that

$$\lim_{m\to\infty} \frac{1}{b^{2m}} \sum_{x\in G} \left(\mathrm{Prob}(g = x) - \frac{1}{n}\right)^2$$

is positive and finite.

2010-A-5. Let G be a group with operation $*$. Suppose that

(i) G is a subset of $\mathbf{R}^3$ (but $*$ need not be related to addition of vectors);

(ii) for each $\mathbf{a}, \mathbf{b} \in G$, either $\mathbf{a} \times \mathbf{b} = \mathbf{a} * \mathbf{b}$ or $\mathbf{a} \times \mathbf{b} = \mathbf{0}$ (or both), where $\times$ is the usual cross product in $\mathbf{R}^3$.

Prove that $\mathbf{a} \times \mathbf{b} = \mathbf{0}$ for all $\mathbf{a}, \mathbf{b} \in G$¿

2009-A-5. Is there a finite abelian group G such that the product of all the orders of its elements is 2^{2009}?

2008-A-6. Prove that there exists a constant $c > 0$ such that in every nontrivial finite group G there exists a sequence of length at most $c \ln |G|$ with the property that each element of G equals the product of some subsequence. (The elements of G in the sequence are not required to be distinct. A *subsequence* of a sequence is obtained by selecting some of the terms , nont necessarily consecutive, without reordering them; for example, 4, 4, 2 is a subsequence of 2, 4, 6, 4, 2 but 2, 2, 4 is not.)

2007-A-5. Suppose that a finite group has exactly n elements of order p, where p is a prime. Prove that either $n = 0$ or p divides $n + 1$.

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 $\phi : G \to G$ a function such that

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

whenever $g_1 g_2 g_3 = e = h_1 h_2 h_3$. 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 $g : A \to \mathbf{R}$ such that $g(a) < g(b) < g(c)$ implies $(a, b, c) \in S$. [Note: $\mathbf{R}$ is the set of real numbers.]

1995-A-1. 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* (notnecessarily 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.

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 $\{a^n : n = 1, 2, 3, \cdots\}$ 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

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

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 $x_1ax_2a \cdots x_na$, 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 $n_1, n_2, \cdots n_k$ 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 componentwise), consider the subgroup H generated by the three elements

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

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.

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.