Abstract algebra

18.A34 Guest Lecture: Fall 2019

Zilin Jiang

September 18, 2019

> This is functional equation at its worst!
>
> ---
>
> a student of 18.A34

1 Sampler

Problem 1 (Putnam 1972 A2). Let S be a set and let $*$ be a binary operation on S satisfying the laws

$$\begin{aligned} x*(x*y) &= y \qquad \text{for all } x, y \text{ in } S, \\ (y*x)*x &= y \qquad \text{for all } x, y \text{ in } S. \end{aligned}$$

Show that $*$ is commutative but not necessarily associative.

Problem 2 (Putnam 1972 B3). 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 $B = 1$.

Problem 3 (Putnam 2018 A4). Let m and n be positive integers with $\gcd(m, n) = 1$, and let

$$a_k = \lfloor mk/n \rfloor - \lfloor m(k-1)/n \rfloor$$

for $k = 1, 2, \ldots, n$. Suppose that g and h are elements in a group G and that

$$gh^{a_1}gh^{a_2}\ldots gh^{a_n} = e,$$

where e is the identity element. Show that $gh = hg$.

Problem 4 (Putnam 1990 B4). Let G be a finite group of order n generated by a and b. Prove or disprove: there is a sequence

$$g_1, g_2, g_3, \cdots, g_{2n}$$

such that

(a) every element of G occurs exactly twice, and

(b) g_{i+1} equals g_ia or g_ib for $i = 1, 2, \ldots, 2n$. (Interpret g_{2n+1} as g_1.)

Problem 5 (Putnam 2016 A5)**.** 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 $m_n, n_1, m_2, n_2, \dots, m_r, n_r \in \{1, -1\}$.

Problem 6 (Kauffman)**.** The cross product in $\mathbb{R}^3$ is not associative, and so $v_1 \times v_2 \times \cdots \times v_n$ is not well-defined if $n > 3$. When we put in enough brackets to make it well-defined, we get a *bracketing.* For every two bracketings of $v_1 \times v_2 \times \cdots \times v_n$, there exists an assignment $v_1, \dots, v_n \in \{e_1, e_2, e_3\}$ such that the evaluations of the two bracketings are equal and nonzero.

2 Problems

Problem 7 (Putnam 1977 B6)**.** 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's in H.

(a) Show that P is a finite set.

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

Problem 8 (Putnam 1984 B3)**.** Prove or disprove the following statement: If F is a finite set with two or more elements, then there exists a binary operation $*$ on F such that for all x, y, z in F,

(i) $x * z = y * z$ implies $x = y$ (right cancellation holds), and

(ii) $x * (y * z) \neq (x * y) * z$ (*no* case of associativity holds).

Problem 9 (Putnam 1987 B6)**.** 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 $a \neq 0$ in F, exactly one of a and $-a$ is in S. Let N be the number of elements in the intersection $S \cap \{2a : a \in S\}$. Prove that N is even.

Problem 10 (Putnam 1989 B2)**.** Let S be a nonempty 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?

Problem 11 (Putnam 1992 B6)**.** Let $\mathcal{M}$ be a set of real $n \times n$ matrices such that

(i) $I \in \mathcal{M}$, where I is the $n \times n$ identity matrix;

(ii) if $A \in \mathcal{M}$ and $B \in \mathcal{M}$, then either $AB \in \mathcal{M}$ or $-AB \in \mathcal{M}$, but not both;

(iii) if $A \in \mathcal{M}$ and $B \in \mathcal{M}$, then either $AB = BA$ or $AB = -BA$;

(iv) if $A \in \mathcal{M}$ and $A \notin I$, there is at least one $B \in \mathcal{M}$ such that $AB = -BA$.

Prove that $\mathcal{M}$ contains at most n^2 matrices.

Problem 12 (Putnam 1996 A4)**.** 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 $(c, b, a) \notin S$ [for a, b, c distinct];

(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 from A to $\mathbb{R}$ such that $g(a) < g(b) < g(c)$ implies $(a, b, c) \in S$.

Problem 13 (Putnam 2007 A5)**.** 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 $n + 1$.

Problem 14 (Putnam 2008 A6)**.** 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, not 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.)

Problem 15 (Putnam 2009 A5)**.** Is there a finite abelian group G such that the product of the orders of all its elements is 2^{2009}?

Problem 16 (Putname 2010 A5)**.** Let G be a group, with operation $*$. Suppose that

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

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

Problem 17 (Putnam 2011 A6)**.** Let G be an abelian group with n elements, and let $\{g_1 = e, g_2, \ldots, g_k\} \subsetneq G$ be a (not necessarily minimal) set of distinct generators of G. A special die, which randomly selects one of the elements $g_1, g_2, \ldots, g_k$ 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.

Problem 18. Let R be a *noncommutative* ring with identity. Suppose that x, y are elements of R such that $1 - xy$ and $1 - yx$ are invertible. (By the previous problem it suffice to assume that only $1 - xy$ is invertible, but this is irrelevant.) Show that

$$(1 + x)(1 - yx)^{-1}(1 + y) = (1 + y)(1 - xy)^{-1}(1 + x). \tag{1}$$

This problem illustrates that "noncommutative high school algebra" is a lot harder than ordinary (commutative) high school algebra.

Note. Formally we have

$$(1 - yx)^{-1} = 1 + yx + yxyx + yxyxyx + \cdots$$

and similarly for $(1 - xy)^{-1}$. Thus both sides of (1) are formally equal to the sum of all "alternating words" (products of x's and y's with no two x's or y's appearing consecutively). This makes the identity (1) plausible, but our formal argument is not a proof.

Problem 19. Let G be a group of order $4n + 2$, $n \geq 1$. Prove that G is not a simple group, i.e., G has a proper normal subgroup.

Problem 20. Let R satisfy all the axioms of a ring except commutativity of addition. Show that $ax + by = by + ax$ for all $a, b, x, y \in R$.

Problem 21. Let G denote the set of all infinite sequences $(a_1, a_2, \dots)$ of integers a_i. We can add elements of G coordinate-wise, i.e.,

$$(a_1, a_2, \dots) + (b_1, b_2, \dots) = (a_1 + b_1, a_2 + b_2, \dots).$$

Let $\mathbb{Z}$ denote the set of integers. Suppose $f\colon \to \mathbb{Z}$ is a function satisfying $f(x+y) = f(x)+f(y)$ for all $x, y \in G$. Let e_i be the element of G with a 1 in position i and 0's elsewhere.

(a) Suppose that $f(e_i) = 0$ for all i. Show that $f(x) = 0$ for all $x \in G$.

(b) Show that $f(e_i) = 0$ for all but finitely many i.

Problem 22. Let G be a finite group, and set $f(G) = \#\{(u, v) \in G \times G : uv = vu\}$. Find a formula for $f(G)$ in terms of the order of G and the number $k(G)$ of conjugacy classes of G. (Two elements $x, y \in G$ are *conjugate* if $y = axa^{-1}$ for some $a \in G$. Conjugacy is an equivalence relation whose equivalence classes are called *conjugacy classes*.)

Problem 23 (difficult)**.** Let n be an odd positive integer. Show that the number of ways to write the identity permutation ι of $1, 2, \dots, n$ as a product $uvw = \iota$ of three n-cycles is $2(n-1)!^2/(n+1)$.

Problem 24. Let G be any finite group, and let $w \in G$. Find the number of pairs $(u, v) \in G \times G$ satisfying $w = uvu^2vuv$.

Problem 25. Show that the number of ways to write the cycle $(1, 2, \dots, n)$ as a product of $n - 1$ transpositions is n^{n-2}. For instance, when $n = 3$ we have (multiplying permutations left-to-right) three ways:

$$(1, 2, 3) = (1, 3)(2, 3) = (1, 2)(1, 3) = (2, 3)(1, 2).$$

Problem 26 (difficult)**.** Let $s_i = (i, i + 1) \in S_n$, i.e., s_i is the permutation of $1, 2, \dots, n$ that transposes i and $i + 1$ and fixes all other j. Let $f(n)$ be the number of ways to write the permutation $n, n-1, \dots, 1$ in the form $s_{i_1} s_{i_2} \cdots s_{i_p}$, where $p = \binom{n}{2}$. For instance, $321 = s_1 s_2 s_1 = s_2 s_1 s_2$, so $f(3) = 2$. Moreover, $f(4) = 16$. Show that $f(n)$ is the number of sequences $a_1, \dots, a_p$ of $n-1$ 1's, $n-2$ 2's, ..., one $n-1$, such that in any prefix $a_1, a_2, \dots, a_k$, the number of $i+1$'s does not exceed the number of i's. For instance, when $n = 3$ there are the two sequences 112 and 121.

Note. An explicit formula is known for $f(n)$, but this is irrelevant here.

Problem 27 (difficult)**.** In the notation of the previous problem, show that

$$\sum_{i_1,i_2,\ldots,i_p} i_1 i_2 \cdots i_p = p!,$$

where the sum is over all sequences $i_1,\ldots,i_p$ for which $n, n-1, \ldots, 1 = s_{i_1} s_{i_2} \cdots s_{i_p}$. For instance, when $n = 3$ we get $1 \cdot 2 \cdot 1 + 2 \cdot 1 \cdot 2 = 3!$.

Note. The only known proofs are algebraic. It would be interesting to give a combinatorial proof.