

PROBLEMS ON ABSTRACT ALGEBRA

1. (68P) A is a subset of a finite group G (with group operation called multiplication), 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 .
2. (69P) 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”?
3. (71P) Let S be a set and let \circ be a binary operation on S satisfying the two laws

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

Show that \circ is associative and commutative.

4. (72P) Let S be a set and let $*$ be a binary operation on S satisfying the laws

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

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

5. (72P) 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 $B = 1$.
6. (76P) 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, \dots, n_k are any integers, and $A^0 = B^0 = 1$ as usual. Also, suppose that $A^4 = B^7 = ABA^{-1}B = 1$, $A^2 \neq 1$, and $B \neq 1$.

(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 .

7. (77P) 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 $x_1ax_2a\cdots x_n a$, 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.

8. (78P) A “bypass” operation on a set S is a mapping from $S \times S$ to S with the property

$$B(B(w, x), B(y, z)) = B(w, z) \quad \text{for all } w, x, y, z \text{ in } S.$$

(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 exist d and e in S with $B(d, e) = d \neq e$.
 - (iii) There exist f and g in S with $B(f, g) \neq f$.

9. (79P) 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 ?

10. (84P) 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).
11. (87P) 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.
12. (89P) 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?
13. (90P) Let G be a finite group of order n generated by a and b . Prove or disprove: there is a sequence

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

such that

- (1) every element of G occurs exactly twice, and
 - (2) g_{i+1} equals $g_i a$ or $g_i b$ for $i = 1, 2, \dots, 2n$. (Interpret g_{2n+1} as g_1 .)
14. (91P) Let P be an odd prime and let \mathbb{Z}_p denote (the field of) integers modulo p . How many elements are in the set

$$\{x^2 : x \in \mathbb{Z}_p\} \cap \{y^2 + 1 : y \in \mathbb{Z}_p\}?$$

15. (92P) 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.

16. (94P) For any integer a , set

$$n_a = 101a - 100 \cdot 2^a.$$

Show that for $0 \leq a, b, c, d \leq 99$, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.

17. (96P) 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 $(a, b, c) \in S$.

18. (97P) 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 $x, y \in G$).

19. (01P) Consider a set S and a binary operation $*$, i.e., for each $a, b \in S$, $a * b \in S$. Assume $(a * b) * a = b$ for all $a, b \in S$. Prove that $a * (b * a) = b$ for all $a, b \in S$.
20. (07P) 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 $n + 1$.
21. (08P) 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.)
22. (09P) Is there a finite abelian group G such that the product of the orders of all its elements is 2^{2009} ?

23. (10P)

Let G be a group, with operation $*$. Suppose that

- (a) G is a subset of \mathbb{R}^3 (but $*$ need not be related to addition of vectors);
- (b) 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 $\mathbf{a}, \mathbf{b} \in G$.

24. (11P) Let G be an abelian group with n elements, and let $\{g_1 = e, g_2, \dots, g_k\} \subsetneq G$ 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, \dots, 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

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

is positive and finite.

25. (12P) 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 $a = b$.

26. Let x, y be elements in a (not necessarily commutative) ring such that $1 - xy$ is invertible. Prove that $1 - yx$ is also invertible.

27. 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

$$(1 + x)(1 - yx)^{-1}(1 + y) = (1 + y)(1 - xy)^{-1}(1 + x). \quad (11)$$

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

NOTE. Formally we have

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

and similarly for $(1 - xy)^{-1}$. Thus both sides of (11) 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 (11) plausible, but our formal argument is not a proof.

28. Let G be a finite group of order n . Suppose that for each prime divisor d of n , there is exactly one subgroup of G of order d . Prove that G is a cyclic group.
29. Prove that there is no nontrivial automorphism of the ring of real numbers. That is, if $f : \mathbb{R} \rightarrow \mathbb{R}$ is a function such that $f(0) = 0$, $f(1) = 1$, $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$, and $f(xy) = f(x)f(y)$ for all $x, y \in \mathbb{R}$, then $f(x) = x$ for all $x \in \mathbb{R}$.
30. (a) Let G be a finitely generated group in which $g^2 = 1$ for each $g \in G$. Prove that G is finite and abelian.
- (b) Let G be a finitely generated group in which $g^3 = 1$ for each $g \in G$. Prove that G is finite.
- (Beware that (b) is hard, while its analogue with 3 replaced by an arbitrary positive integer is in fact false!)
31. Let G be a group of order $4n + 2$. Prove that G is not a simple group, i.e., G has a proper normal subgroup.
32. Let R be a noncommutative ring with identity. Show that if an element $x \in R$ has more than one right inverse (i.e., there is more than one $y \in R$ such that $xy = 1$), then x has infinitely many right inverses.
33. Let R be a ring for which $x^2 = 0$ for all $x \in R$. Show that $xyz + xzy = 0$ for all $x, y, z \in R$.
34. Let R satisfy all the axioms of a ring except commutativity of addition. Show that $ax + by = by + ax$ for all $a, b, x, y \in R$.
35. How many $n \times n$ matrices of rank r are there over the finite field \mathbb{F}_q ?
36. 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 $f : G \rightarrow \mathbb{Z}$ is a function satisfying $f(x + y) = f(x) + f(y)$ for all $x, y \in G$.

- (a) Let e_i be the element of G with a 1 in position i and 0's elsewhere. Suppose that $f(e_i) = 0$ for all i . Show that $f(x) = 0$ for all $x \in G$. (NOTE. From the fact that f preserves the sum of two elements it follows easily that f preserves *finite* sums. However, it does not necessarily follow that f preserves *infinite* sums.)
- (b) Show that $f(e_i) = 0$ for all but finitely many i .
37. 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*.)

38. (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 $2(n-1)!^2/(n+1)$.
39. Let G be any finite group, and let $w \in G$. Find the number of pairs $(u, v) \in G \times G$ satisfying $w = uvu^2vuv$.
40. 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:

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

41. (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, $321 = s_1s_2s_1 = s_2s_1s_2$, 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, \dots , 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.

42. (difficult) In the notation of the previous problem, show that

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

where the sum is over all sequences i_1, \dots, i_p for which $n, n-1, \dots, 1 = s_{i_1}s_{i_2}\cdots s_{i_p}$. 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.