Abstract Algebra

1. (1968, B-2)* 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. (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"?

3. (1971, B-1)* Let S be a set and let $\circ$ be a binary operation on S satisfying the two laws
$$x \circ x = x \quad \text{for all } x \text{ in } S, \text{ and}$$
$$(x \circ y) \circ z = (y \circ z) \circ x \quad \text{for all } x, y, z, \text{ in } S.$$
Show that $\circ$ is associative and commutative.

4. (1972, A-2) Let S be a set and let $*$ be a binary operation on S satisfying the laws
$$x * (x * y) = y \qquad \text{for all } x, y \text{ in } S,$$
$$(y * x) * x = y \qquad \text{for all } x, y \text{ in } S.$$
Show that $*$ is commutative but not necessarily associative.

5. (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 $B = 1$.

6. (1975, B-1)* In the additive group of ordered pairs of integers (m, n) [with addition defined componentwise: $(m, n) + (m', n') = (m + m', n + n')$] consider the subgroup H generated by the three elements $(3, 8)$, $(4, -1)$, $(5, 4)$. Then H has another set of generators of the form $(1, b)$, $(0, a)$ for some integers a, b with $a > 0$. Find a.

   [Elements $g_1, \ldots, g_k$ are said to *generate* a subgroup H if (i) each $g_i \in H$, and (ii) every $h \in H$ can written as a sum $h = n_1g_1 + \cdots + n_kg_k$ where the n_i are integers (and where, for example, $3g_1 - 2g_2$ means $g_1 + g_1 + g_1 - g_2 - g_2$).]

7. (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 $n_1, \ldots, n_k$ 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.

8. (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
$$x^2 + bx + c, \qquad b, c \in F.$$
For how many elements k in F is $p(x) + k$ irreducible over F?

9. (1984, B-3)*** 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,

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

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

Hints:

1. Consider the multiplication table of the group and use that each row contains each element of the group exactly once.

2. Consider the cardinality of a proper subgroup.

3. Note that the second condition has a third equal expression by cyclically shifting x, y, and z. To show commutativity consider the expression $(x \circ y) \circ (x \circ y)$, then use commutativity to show associativity.

4. To show commutativity, multiply the first equation by $x * y$ from the right and use the second equation. Swap the roles of x and y in the result to get an alternate form of the LHS of the first equation, then multiply it by x from the left. To get a counterexample for associativity, try to find it on a set of three elements.

5. Show that both A and B can be expressed as powers of BA^2, so they commute.

6. Find the smallest positive a such that $(0, a)$ is generated by the given three elements.

7. Using the property $ABA^{-1}B = 1$, show that every element of the group can be written as $A^n B^k$ and find how to multiply two elements of that form.

8. Show that there are $(m - 1)/2$ squares in F, and use the fact that a quadratic polynomial is irreducible iff it has no roots.

9. Try to find examples for small number of elements, then generalize it.