

ALGEBRA

Problems 1 and 2 are required. Choose any three problems from problems 3-6. Specific instructions accompany each problem.

1. Give, with details, counterexamples which show that each of the following statements is false as it stands. Then correct each statement by suitably modifying the underlined phrase.
- If  $D$  is a division ring (= skew field), then a polynomial of degree  $n$  over  $D$  has at most  $n$  roots in  $D$ .
  - If  $A$  is a unique factorization domain, then the greatest common divisor  $d$  of two elements  $a, b \in A$  can be expressed in the form  $d = ax + by$  with suitable elements  $x, y$  of  $A$ .
  - In a commutative ring with unity, every power of a prime ideal is a primary ideal.
  - The alternating group  $A_n$  (the group of even permutations of  $n$  objects) is simple for every natural number  $n$ .
  - Given an  $n \times n$  matrix  $M$ , whose minimal polynomial is of degree  $n$ , there exists a non-singular matrix  $T$  such that  $TMT^{-1}$  is a diagonal matrix. (The coefficients of these matrices are all taken from the field of complex numbers.)
  - The polynomial  $1 + x + x^2 + \dots + x^{n-1}$  is irreducible over the rational numbers for every natural number  $n$ .
  - The normal subgroups of any finite group form a distributive lattice.
  - If a module satisfies the descending chain condition, it satisfies the ascending chain condition.
  - In a commutative ring, every maximal ideal is a prime ideal.
  - If  $G$  is a finite group of order  $g$ , and  $n$  is an integer dividing  $g$ , then  $G$  possesses a subgroup of order  $n$ .
2. Do one of (a), (b) or (c).
- (Two parts) Let  $G$  be a group, and let  $A, B$  be subgroups of finite orders  $m$  and  $n$  respectively. Let  $r$  be the order of the intersection  $A \cap B$ .
    - Show that there exist exactly  $\frac{mn}{r}$  distinct elements of  $G$  which can be written in the form  $ab$  with  $a \in A, b \in B$ .

- ii) Show that if in (i), the order of  $G$  is the least common multiple of  $m$  and  $n$ , then  $r$  is the greatest common divisor of  $m$  and  $n$ , and every element of  $G$  has the form  $ab$  with  $a \in A$ ,  $b \in B$ .
- b) Let  $G$  be the direct sum of the group of integers and a finite cyclic group. Describe all of the automorphisms of  $G$ .
- c) Let  $G$  be a group and let  $N_1, \dots, N_r$  be maximal, proper, normal, subgroups of  $G$  such that no one of them contains the intersection of the others. Establish an isomorphism

$$G / \bigcap_{j=1}^r N_j \cong (G/N_1) \times (G/N_2) \times \dots \times (G/N_r).$$

3. Do one of (a), (b) or (c).

- a) Let  $\alpha, \beta$  be complex numbers such that  $\alpha^3 + 3\alpha + 5 = 0$ ,  $\beta^5 + 7\beta + 7 = 0$ . Prove that the equation

$$\alpha^2 + (11\beta^4 - 13\beta^2 + 17)\alpha + 19\beta^3 - 23\beta = 0$$

is false.

- b) Let  $\Omega$  be an extension field of a field  $K$ , and suppose that  $A, B$  are two subfields of  $\Omega$  which are both normal and separable of finite degree over  $K$ , and which have intersection  $K$ . Show that the compositum  $(A, B)$  obtained by simultaneous adjunction of  $A$  and  $B$  to  $K$  is normal, separable, of finite degree over  $K$ , and that its Galois Group is isomorphic to the direct product of the Galois Groups of  $A$  and  $B$  over  $K$ .
- c) (3 parts) Let  $K$  be a field of characteristic  $\neq 2$ . Let  $a \in K$ , and let  $\Omega$  be a splitting field over  $K$  of the polynomial  $x^4 - a$ .
- i) Show that  $\Omega/K$  is separable, that  $\Omega$  contains an element  $i$  such that  $i^2 = -1$ , and that the degree  $[\Omega:K]$  is at most 8.
- ii) Prove that  $[\Omega:K] = 8$  if and only if neither  $a$  nor  $-a$  nor  $-1$  is a square in  $K$ .
- iii) Prove that if  $[\Omega:K] = 8$ , then the Galois Group of  $\Omega/K$  is isomorphic to the group of symmetries of a square.

4. Do one of (a), (b) or (c).

- a) Prove that the field  $\mathbb{C}$  of complex numbers has infinitely many automorphisms, and that the only elements of  $\mathbb{C}$  left fixed by all the automorphisms are the rational numbers.

- b) Let  $A$  be a commutative ring with unity, and let  $A[X]$  be the polynomial ring in one variable over  $A$ . If  $p(X) \in A[X]$  is a zero divisor, show that there is an  $a \neq 0$ ,  $a \in A$ , such that  $a \cdot p(X) = 0$ . (Hint: Choose  $g(x)$  of minimal degree such that  $g(X)p(X) = 0$ .)
- c) Let  $A$  be a commutative ring with unity, and let  $X_1, \dots, X_n$  be independent indeterminates over  $A$ . Let  $B = A[[X_1, \dots, X_n]] =$  ring of formal power series in  $n$  variables over  $A$ . Show that  $B$  possesses exactly one maximal ideal if and only if  $A$  possesses exactly one maximal ideal.
5. Do one of (a), (b) or (c).
- a) Let  $V$  be a finite dimensional vector space over an algebraically closed field, say  $C$ . The question - Is a given linear transformation  $A$  on  $V$  diagonalizable (i.e., has a diagonal matrix in a suitable basis of  $V$ )? - can be decided by means of rational operations alone; i.e., without solving algebraic equations of degree  $> 1$ . Indicate how.
- b) Let  $V$  be a finite dimensional vector space over the field of real numbers, and let  $F_1, F_2$  be two quadratic forms such that  $F_1$  is positive definite and  $F_2$  is non-negative but not identically zero. Show that the determinant of  $F_1 + F_2$  is larger than the determinant of  $F_1$ .
- c) Let  $V$  be a vector space over a field  $k$  of characteristic  $p > 0$ .  $V$  is said to be a restricted, abelian, Lie algebra over  $k$  if it has in addition a map  $\varphi : V \rightarrow V$  satisfying

$$\varphi(v+w) = \varphi(v) + \varphi(w)$$

$$\varphi(av) = a^p \varphi(v) \quad (a \in k).$$

A subspace  $W \subseteq V$  is a sub-Lie algebra if and only if  $\varphi(W) \subseteq W$ .  $V$  is called simple if it has no non-trivial sub-Lie algebras. Prove: A simple, restricted, abelian, Lie algebra is finite dimensional as vector space over  $k$ .

6. Do one of (a), (b) or (c).
- a) Let  $A$  be a noetherian ring,  $M$  an  $A$ -module, and assume  $M \neq (0)$ . Show that there is a prime ideal  $P$  of  $A$  such that  $A/P$  is isomorphic (as  $A$ -module) to a submodule of  $M$ .

- b) Let  $A$  be a commutative ring, and let  $f(X) = a_0 + a_1X + \dots + a_nX^n$  be a polynomial in  $A[X]$ . Show that  $f(X)$  is invertible in  $A[X]$  if and only if  $a_0$  is invertible in  $A$  and  $a_j$  is nilpotent for  $j = 1, \dots, n$ .
- c) Let  $A$  be a noetherian ring in which every non-zero prime ideal is maximal. (For example,  $\mathbb{Z}$ .) Let  $\mathfrak{U}$  be an ideal of  $A$ . Show that  $\mathfrak{U}$  is a finite product of primary ideals.