

# Algebra Problems

Math 504 – 505

Jerry L. Kazdan

- Show that  $\sqrt{2}$  is not a rational number.
  - Show that  $\sqrt{3}$  is not a rational number.
- Prove that there are infinitely many prime numbers.
  - Prove that there are infinitely many primes of the form  $4n + 3$  (the  $4n + 1$  case is more difficult).
- Let  $\mathbf{u} \times \mathbf{v}$  denote the cross product in  $\mathbb{R}^3$ . For a fixed vector  $\mathbf{u}$ , for which vectors  $\mathbf{z}$  can one solve  $\mathbf{u} \times \mathbf{v} = \mathbf{z}$  for  $\mathbf{v}$ ? To what extent is the solution unique?
- If  $x$  and  $y$  are real numbers, show that the set of matrices of the form  $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$  is isomorphic to the field of complex numbers  $z = x + iy$ .
- Consider the matrix  $M = \begin{bmatrix} 1 & -1 \\ 2 & -1 \end{bmatrix}$ .
  - Is there a real invertible matrix  $P$  such that  $PAP^{-1}$  is a real diagonal matrix? If so, find  $P$ . If not, state why not.
  - Is there a complex invertible matrix  $P$  such that  $PAP^{-1}$  is a complex diagonal matrix? If so, find  $P$ . If not, state why not.
  - Think of the elements of  $M$  as belonging to the finite field  $\mathbf{Z}/5\mathbf{Z}$ . Is there an invertible matrix  $P$  with entries in this finite field such that  $PAP^{-1}$  is a  $\mathbf{Z}/5\mathbf{Z}$ -valued diagonal matrix? If so, find  $P$ . If not, state why not.
- Suppose that for a polynomial  $p \in \mathbb{Z}[x]$  we have  $p(2003) = 2003$ . Show that  $p$  can have at most three different integer roots. [REMARK: 2003 is a prime number.]
- The *quaternions* can be defined as expressions of the form  $q = x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$ , where  $x, y, z,$  and  $w$  are real numbers. They are added as vectors and multiplied using the rules  $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ ,  $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$ ,  $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$ ,  $\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$  and the usual distributive rules. Define the *conjugate* by  $\bar{q} = x - y\mathbf{i} - z\mathbf{j} - w\mathbf{k}$ .
  - Compute  $q\bar{q}$ . Use this to show that every  $q \neq 0$  has a multiplicative inverse. Thus show that the quaternions are a field, except they are not commutative under multiplication.

b) Prove that the *unit quaternions*, that is, those  $q$  with  $x^2 + y^2 + z^2 + w^2 = 1$  form a group under multiplication, and that this group is isomorphic to  $SU_2$ . Note that clearly the unit quaternions can also be thought of as points on the unit sphere  $S^3 \in \mathbb{R}^4$ .

c) Let

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}.$$

Show that the set of matrices of the form  $Q = x\mathbf{I} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$  is isomorphic to the quaternions.

8. Consider the ring whose elements are

$$q = a + bi + cj + dk, \quad \text{where} \quad i^2 = j^2 = k^2 = -1, \quad ij = -ji = k,$$

with  $a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$ , where  $p$  is a prime.

Show that this ring is isomorphic to the ring of  $2 \times 2$  matrices  $\mathbb{Z}/p\mathbb{Z}$  if  $p$  is odd but *not* if  $p = 2$ .

9. Let  $G$  be a finite group of order  $n$  and  $H$  a subgroup of order  $k$ .

a) Prove that  $n$  is divisible by  $k$ .

b) Conversely, if  $n$  is divisible by  $k$ , must  $G$  have a subgroup of order  $k$ ? Proof or counterexample.

10. Let  $p$  be a prime number and  $G = \mathbb{Z}/p\mathbb{Z}$ . Find the total number of group homomorphisms  $G \times G \rightarrow G \times G$ .

11. If  $G$  is a finite group and  $x, y \in G$ , then  $o(xy) = o(yx)$ . Proof or counterexample.

12. Let  $G$  be a finite abelian group of odd order. Prove that the product of all the elements of  $G$  is the identity.

13. a) Let  $p(x)$  be a polynomial with real coefficients. If  $z \in \mathbb{C}$  is a root, show that  $\bar{z}$  is also a root.

b)  $p(x)$  be a polynomial with integer coefficients. If  $x = 5 + 2\sqrt{3}$  is a root, show that  $x = 5 - 2\sqrt{3}$  is also a root.

14. Suppose that  $H$  is a non-trivial subgroup of the additive group  $(\mathbb{R}, +)$  of real numbers.

- a) Show that either (i)  $H$  is infinite cyclic, or (ii) for any  $\varepsilon > 0$ , there is an  $x \in H$  with  $0 < x < \varepsilon$ .
- b) If  $H$  is infinite cyclic, prove that  $\mathbb{R}/H$  is isomorphic to the multiplicative group  $S^1 = \{z \in \mathbb{C} : |z| = 1\}$  of complex numbers of modulus 1.
15. Suppose  $G$  is a finite group,  $H$  is a normal subgroup of  $G$ , and  $P$  is a Sylow subgroup of  $H$ . Prove that  $G = H \cdot N_G(P)$ .
16. In each case, decide whether the two groups are isomorphic:
- a)  $(\mathbb{Z}, +)$  and  $(\mathbb{Q}, +)$                       c)  $(\mathbb{Q}, +)$  and  $(\mathbb{Q}_{>0}, \cdot)$   
b)  $(\mathbb{R}, +)$  and  $(\mathbb{R}_{>0}, \cdot)$                       d)  $(\mathbb{R}^*, \cdot)$  and  $(\mathbb{C}^*, \cdot)$
17. Suppose  $a, b, c \in \mathbb{Q}$  are such that  $a + b + c$ ,  $ab + bc + ca$  and  $abc$  are all integers. Prove that  $a$ ,  $b$  and  $c$  are integers. Can you generalize this?
18. Suppose  $f(x) = ax^2 + bx + c$  has real coefficients and no real roots. Prove that the quotient ring  $\mathbb{R}[x]/(f(x))$  is isomorphic to the field of complex numbers  $\mathbb{C}$ .
19. Suppose we are given a surjective ring homomorphism from the polynomial ring  $\mathbb{C}[x]$  onto an integral domain  $R$ . Prove that  $R$  is isomorphic to either  $\mathbb{C}[x]$  or  $\mathbb{C}$ .
20. Let  $k, n \in \mathbb{N}$  How many group homomorphisms are there from  $\mathbb{Z}/k\mathbb{Z}$  to  $\mathbb{Z}/n\mathbb{Z}$ ? Justify your assertions.
21. Let  $G$  be a group and let  $H$  be the subgroup generated by all elements of order 2 in  $G$ . Show that  $H$  is normal in  $G$ . [Note: If  $S = \emptyset$ , remember group generated by  $S = \{1\}$ .]
22. Let  $G$  be a finite group and suppose  $G$  possesses a (normal) subgroup  $H$  with the two properties
- a).  $(G : H) = 2$   
b).  $H$  has odd order
- Show directly (no Sylow, no Cauchy) that  $G$  has an element exactly of order 2.
23. Suppose  $G$  is a group in which each element ( $\neq 1$ ) has order 2. Prove that  $G$  is abelian.

24. (variant of the previous problem) Let  $G$  be a non-abelian group of order  $2^k$  for some integer  $k \geq 3$ . Prove that  $G$  has an element of order 4 (no Sylow, no Cauchy).
25. Let  $G$  be a finite group and let  $\Phi$  be the intersection of all the maximal subgroups of  $G$ . Suppose that there exists an element  $\sigma \in G$  such that  $\sigma$  together with  $\Phi$  generates all of  $G$ . Show that  $G$  is a cyclic group.
26. Let  $\phi(n)$  be the number of integers  $q$  with  $1 \leq q \leq n-1$  such that  $q$  is relatively prime to  $n$ .
- If  $(k, n) = 1$ , show that  $\phi(kn) = \phi(k)\phi(n)$ .
  - If  $p$  is prime, show  $\phi(p^a) = p^{a-1}(p-1)$
27. Let  $G$  be a finite group of order  $g$ , and let  $M$  be a minimal non-trivial subgroup of  $G$ . Show that  $M$  is cyclic of prime order  $p$ . Show further that  $p \mid g$ .
28. Let  $A_4$  be the alternating group on four letters. It has order 12. Prove that it has no subgroup of order 6.
29. Prove that a group is abelian if and only if the map  $\phi : a \mapsto a^{-1}$  is an isomorphism.
30. If  $G$  is a group of odd order, show that the map  $\phi(a) = a^{-1}$  has precisely one fixed point. [Remark: The converse is also true, but harder.]
31. Let  $\psi$  be an automorphism of a group  $G$ . Write  $\text{Fix}(\psi)$  for the set of fixed points of  $\psi$ , that is,
- $$\text{Fix}(\psi) = \{\sigma \in G \mid \psi(\sigma) = \sigma\}.$$
- Show that  $\text{Fix}(\psi)$  is a subgroup of  $G$ .

32. Let  $G$  be a finite group and let  $S$  be a non-empty subset of  $G$ . Write

$$Z(S) = \{\sigma \in G \mid \sigma s = s\sigma \text{ for all } s \in S\}$$

$$N(S) = \{\tau \in G \mid \tau s \tau^{-1} \subseteq S \text{ for all } s \in S\}.$$

Then  $Z(S)$  and  $N(S)$  are sub-groups of  $G$ .

- Show that  $Z(S) \subseteq N(S)$  and
- $Z(S)$  is a normal subgroup of  $N(S)$ .

33. If  $G$  is a finite group of order  $g$ , and if for each  $\sigma \in G$  we have an  $n \times n$  invertible matrix (over  $\mathbb{C}$ ), say  $T(\sigma)$ , in such a way that  $T(\sigma\tau) = T(\sigma)T(\tau)$ , show that every eigenvalue of each  $T(\sigma)$  is a  $g^{\text{th}}$  root of unity.

34. Let  $f(x)$  be a monic polynomial with real coefficients. Say

$$f(x) = p_1(x) \cdots p_k(x)$$

is a factorization of  $f$  into monic irreducible polynomials with real coefficients (repetitions are permitted). Prove that each  $p_j(x)$  has one of the forms

$$x - \alpha \quad \text{or} \quad x^2 - \beta x + \gamma,$$

where  $\alpha$ ,  $\beta$ , and  $\gamma$  are real numbers.

35. Let  $f(x)$  be an irreducible polynomial with rational coefficients, and let  $f'(x)$  be its derivative. Show that there exist two polynomials  $p(x)$ ,  $q(x)$  with rational coefficients such that

$$p(x)f(x) + q(x)f'(x) = 1.$$

Illustrate this for  $f(x) = x^3 - 3x + 1$ .

36. Let  $G$  be an abelian group and suppose that  $T$  is a homomorphism of  $G$  to the group  $GL(n)$  of  $n \times n$  invertible complex matrices. Suppose that for some  $\sigma \in G$  the non-zero vector  $v$  is an eigenvector of the matrix  $T(\sigma)$  with corresponding eigenvalue  $\lambda$ .

a) Show that  $\lambda \neq 0$ .

b) Show that for each  $\tau \in G$ , the vector  $T(\tau)v$  is also an eigenvector of  $T(\sigma)$  with the same eigenvalue  $\lambda$ .

37. a) If  $p_1, \dots, p_n$  are  $n$  given integers and if  $(p_1, \dots, p_n)$  appears as a row of an  $n \times n$  integer matrix of determinant 1, show that the  $p_j$  have no non-trivial common factor.

b) Prove the converse in the case  $n = 2$ , that is, if  $p_1$  and  $p_2$  are relatively prime, then  $(p_1, p_2)$  appears as a row of a  $2 \times 2$  integer matrix whose determinant is 1.

38. Let  $\sigma$  be an element of a group and assume the order of  $\sigma$  is finite, say  $n$ . Write  $\tau = \sigma^\ell$ . Show that  $\sigma$  and  $\tau$  have the same order if and only if  $(\ell, n) = 1$ .

39. Let  $f(x) = x^3 - ax + 1$ , where  $a$  is an integer. Prove that  $f(x)$  is irreducible over the rationals provided  $a \neq 0$  or  $a \neq 2$ . Further, in the cases  $a = 0$  and  $a = 2$ , give the factorization of  $f(x)$ .
40. Let  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$  be a polynomial with complex coefficients. Show that by a linear substitution  $y = x - \alpha$  for some  $\alpha \in \mathbb{C}$  the polynomial  $f(x)$  transforms to  $g(y) = y^n + b_{n-2}y^{n-2} + \cdots + b_0$  with no  $y^{n-1}$  term. Find  $\alpha$  explicitly in terms of the coefficients of  $f$ .
41. Let  $G$  be a finite group and write  $Z$  for the center of  $G$ , that is, the subgroup of all elements of  $G$ . Prove that the index  $(G : Z)$  is *never* a prime number. [An easier version is to prove that  $(G : Z) \neq 2$ .]
42. Give (with proof) an example of a commutative ring  $R$  and an ideal  $I$  in  $R$  which cannot be generated by one element.
43. Let  $\sigma$  be an element of a group  $G$  and suppose that  $\sigma$  has order  $n$ . Write  $n = ab$  with  $(a, b) = 1$ . Show there exist unique elements  $\rho, \tau \in G$  with  $\rho$  of order  $a$  and  $\tau$  of order  $b$  such that  $\sigma = \rho\tau = \tau\rho$ .
44. Let  $G$  be the multiplicative group of  $2 \times 2$  integer matrices with determinant 1. Find  $\sigma, \tau \in G$  with  $\sigma^4 = \tau^6 = 1$  and  $G$  generated by  $\sigma$  and  $\tau$ . Show further that  $\sigma\tau$  has infinite order.
45. For a finite group  $G$ , write  $\mathbb{Z}[G]$  for the set of formal linear combinations

$$\sum_{\sigma \in G} \lambda_{\sigma} \sigma, \quad \text{where } \lambda_{\sigma} \in \mathbb{Z}.$$

Add these component-wise and multiply by using the group law and distributivity. There is a map from the ring  $\mathbb{Z}[G]$ , so obtained, to  $\mathbb{Z}$ , namely

$$\sum_{\sigma \in G} \lambda_{\sigma} \sigma \mapsto \sum_{\sigma \in G} \lambda_{\sigma}.$$

This is a ring homomorphism. Let  $I$  be its kernel. Show that  $I$  is generated as an ideal by all elements  $\{\sigma - 1, \sigma \in G\}$ .

46. Let  $G$  be a group generated by two elements  $\sigma, \tau$ . Suppose that  $\sigma^3 = \tau^3 = 1$ . Prove that  $\tau\sigma\tau^{-1} \neq \sigma^{-1}$ .

47. Let  $\mathbb{N} = \{1, 2, 3, \dots\}$  and write  $\Sigma$  for the group of all one-to-one maps of  $N$  onto itself having the property:

If  $\phi \in \Sigma$  there is some  $n = n(\phi)$  such that  $m > n$  implies  $\phi(m) = m$ .

Find all the normal subgroups of  $\Sigma$ .

48. For positive integers  $n$  and  $k$ , define  $d_k(n) = \begin{cases} 1 & \text{if } n \nmid k \\ 1 - n & \text{if } n \mid k \end{cases}$ . Show that

$$\sum_{k=1}^{\infty} \frac{d_k(n)}{-k} = \log n \quad (n > 1).$$

49. Let  $\alpha$  be a complex number with the following two properties:

- $\alpha$  is a root of  $X^n + a_1X^{n-1} + \dots + a_n = 0$ , where the coefficients are integers.
- There is a prime number  $p$  so that  $p\alpha$  is an integer.

Show that  $\alpha$  is an integer.

50. For each of the statements below give an example with details or a short statement why such an example cannot exist.

- A non-cyclic group of order 289 whose center is cyclic.
- If  $p$  is a prime number, a finite field with  $2p^3$  elements.
- An infinite abelian group all of whose (proper) subgroups are finite.
- A ring with no two-sided ideals but with many left ideals.
- A vector space  $V$  over a field  $k$  so that  $V$  has 100 elements.

51. Give examples of the following:

- A finite commutative group that is not cyclic.
- A commutative ring (that is not a field) with finitely many elements.
- A commutative ring (that is not a field) with infinitely many elements.
- A non-commutative ring with infinitely many elements.
- A non-commutative ring with finitely many elements.

52. For each of the statements below give an example with details or a short statement why such an example cannot exist.

- a) For each integer  $n \geq 1$ , a polynomial  $p(x)$  of degree  $n$  (with rational coefficients) that is irreducible over the rational numbers.
- b) A non-abelian group all of whose subgroups are normal.
- c) A non-abelian group all of whose proper subgroups are abelian.
- d) A field  $k$  in which every homogeneous polynomial in two variables and having degree  $d > 1$  has a non-trivial zero. [Here “homogeneous” means for some integer  $j$  we have  $f(cx, cy) = c^j f(x, y)$  for all  $c \in k$  while a non-trivial zero means  $f(\xi, \eta) = 0$  for some  $\xi, \eta$ , at least one of which is not zero.]
- e) A finite group  $G$  of order  $g$  and a positive integer  $h$  so that  $h \mid g$  but  $G$  has no subgroup of order  $h$ .
53. Let  $R$  be a PID with the property that there exists a ring homomorphism  $\phi : R \rightarrow \mathbb{Z}$ . Prove that  $\phi$  is an isomorphism. [Note: Part of the hypothesis is that  $\phi(1) = 1$ .
54. Prove that the additive group of rational numbers has no proper maximal subgroup.
55. Let  $G$  be a finite group and let  $M_1, \dots, M_n$  be the list of all its maximal subgroups. Write  $H$  for the intersection  $H = M_1 \cap \dots \cap M_n$ .
- a)  $H \triangleleft G$ .
- b) If an element  $\sigma \in G$  together with the elements of  $H$  generate  $G$ , then  $G$  is a cyclic group.
56. Suppose that  $a, b$  and  $c$  are rational numbers satisfying  $a + b\sqrt{2} + c\sqrt{3} = 0$ . Prove that  $a = b = c = 0$ .
57. a) Let  $G$  be a finite group such that  $G/C(G)$  is cyclic. Here  $C(G)$  denotes the center of  $G$ . Show that  $G$  is abelian.
- b) Show that any group of order  $p^2$  where  $p$  is prime is abelian.
58. Let  $T : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  be a linear transformation such that  $T(v) \perp v$  for any  $v \in \mathbb{R}^3$ . Show that  $T$  is anti-symmetric.
59. Let  $F$  be a field with 17 elements.
- a) How many roots does the equation  $x^5 = 1$  have in  $F$ ?
- b) How many roots does the equation  $x^4 = 1$  have in  $F$ ?

60. Give an example of a polynomial ring with invertible elements of positive degree.
61. Does the polynomial  $x^{12} - 3x^8 + 1$  have multiple complex roots?
62. Let  $G$  be the group of isometries of the three dimensional euclidian space which stabilize a given cube.
- What is the cardinality of  $G$ ?
  - Is  $G$  simple? (In other words, does  $G$  have a non-trivial normal subgroup?)
  - Does  $G$  have an element of order 12?
63. Prove that the multiplicative group of non-zero real numbers does not have a subgroup of index 3.
64. Denote by  $M$  the ring of  $5 \times 5$  matrices with integer elements.
- Does  $M$  have a subring isomorphic to  $\mathbb{Z}[x]$ , the ring of one-variable polynomials with integer coefficients?
  - Does  $M$  have a subring isomorphic to the factor ring of  $\mathbb{Z}[x]$  modulo the ideal generated by  $x^3(x-1)^2$ ?
65. Does the ring of  $3 \times 3$  matrices over the reals contain a subring isomorphic to
- the field of complex numbers?
  - the division ring of quaternions?
66. Compute the endomorphism ring of the additive group  $Q^+$  of rationals. Does  $Q^+$  contain maximal subgroups?
67. If  $F$  is a division ring such that the multiplicative group of nonzero elements of  $F$  is a finite direct sum of cyclic groups, then  $F$  is a finite field.
68. Let  $G$  be the rotation group of a cube.
- What is the cardinality of  $G$ ?
  - Is  $G$  isomorphic to a symmetric group  $S_n$  for some  $n$ ?
69. Suppose that for a polynomial  $p \in \mathbb{Z}[x]$  we have  $p(2003) = 2003$ . Show that  $p$  can have at most three different integer roots. [REMARK: 2003 is a prime number.]

70. Let  $\mathbb{Z}_2$  denote the field of residue classes modulo 2 and consider the four factor rings:

a).  $R_1 = \mathbb{Z}_2[x]/(x^3 + x^2)$

c).  $R_3 = \mathbb{Z}_2[x]/(x^3 + x^2 + 1),$

b).  $R_2 = \mathbb{Z}_2[x]/(x^3 + x^2 + x)$

d).  $R_4 = \mathbb{Z}_2[x]/(x^3 + x^2 + x + 1)$

Determine:

- a) Which (if any) of them contain(s) nonzero nilpotent elements?
- b) Which (if any) of them contain(s) zero divisors?
- c) Which (if any) of them form(s) a field?
- d) Whether any two of these rings are isomorphic to each other.

71. Decompose the group algebras  $Q(\mathbb{Z}_4)$  and  $C(\mathbb{Z}_4)$  into direct sums of their indecomposable ideals, i.e., decompose  $F[g]$  into a direct sum of its indecomposable ideals where  $g$  is the image of  $x$  in the factor ring  $F[x]/(x^4 - 1)$  and  $F$  is a field  $Q$  or  $C$  of either rational or complex numbers, respectively.

72. Describe all groups of order 6.

73. Let  $\mathbb{Z}_2$  denote the field of residue classes modulo 2 and consider the four factor rings:

a).  $R_1 = \mathbb{Z}_2[x]/(x^3 + x^2)$

c).  $R_3 = \mathbb{Z}_2[x]/(x^3 + x^2 + 1),$

b).  $R_2 = \mathbb{Z}_2[x]/(x^3 + x^2 + x)$

d).  $R_4 = \mathbb{Z}_2[x]/(x^3 + x^2 + x + 1)$

Determine:

- a) Which (if any) of them contain(s) nonzero nilpotent elements?
- b) Which (if any) of them contain(s) zero divisors?
- c) Which (if any) of them form(s) a field?
- d) Whether any two of these rings are isomorphic to each other.

74. If a polynomial  $p(x_1, \dots, x_n)$  is the square of a rational function  $r(x_1, \dots, x_n)$ , show that  $r$  must itself be a polynomial.

[Last revised: August 25, 2003]