Chapter 1

Groups

1.1 General Group Theory

KNOW BASIC DEFINITIONS: groups (subgroups, normal and characteristic subgroups, quotients; simple, abelian, solvable, nilpotent groups; commutators, normalizers, centralizers); order, index; homomorphisms (iso, mono, epi, auto, inner); group actions, transitive, orbits, stabilizers, fixed points.

KNOW THE FOLLOWING THEOREMS: the three isomorphism theorems, the correspondence theorem (for subgroups of G/N); Lagrange's theorem, the product formula for $|AB|$; the fundamental theorem for finitely generated abelian groups (see Section 1.3 below); automorphisms of cyclic groups; theorems about p-groups (nilpotency; groups of order p^2 are abelian); Cauchy's theorem; the Sylow theorems (see Section 1.2 below).

KNOW SOLVABILITY AND NILPOTENCY: If $N \lhd G$ then G is solvable if and only if G/N and N are solvable. Solvability chain of derived groups $G^{(n)}$, where $G^{(0)} := G$, $G^{(n+1)} := [G^{(n)}, G^{(n)}]$. The (lower) central series $G^{[n]}$, where $G^{[0]} := G$, $G^{[n+1]} := [G^{[n]}, G]$. Subgroups and quotients of solvable/nilpotent groups are solvable/nilpotent. A nilpotent group has non-trivial center $Z(G)$. If G/N is nilpotent for $N \leq Z(G)$, then also G is nilpotent. If H is a proper subgroup of a nilpotent group G, then $N_G(H) \neq H$.

KNOW THE FOLLOWING CONSTRUCTIONS: direct and semidirect products, "inner" and "outer" version, characterizations when a group is a (semi)direct product of two subgroups.

KNOW THE FOLLOWING CLASSES OF EXAMPLES: cyclic groups and their subgroup structure; symmetric groups S_n, cycle decompositions, conjugation of cycles, the sign function, alternating groups A_n; dihedral groups D_{2n}; the quaternion group; general linear groups $GL_n(F)$ (F a field) and related groups (like $SL_n(F)$).

KNOW GROUP ACTIONS: If a group G acts on a set S then
1. S is the disjoint union of orbits.
2. $|\text{Orbit}(s)| = [G : G_s]$.
3. $|\text{Conjugacy class}(x)| = [G : C_G(x)]$.
4. Class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)],$$

where $x_1, \ldots, x_m$ are representatives of all distinct conjugacy classes in G consisting of more than one element.
5. If G is p-group and S is finite, then $|\text{fixed points}| \equiv |S| \pmod{p}$.

AVOID THE FOLLOWING MISTAKES (incomplete list!): being normal is **not** a transitive relation; $\text{ord}(gh)$ is usually (for nonabelian groups) **not** related to $\text{ord}(g)$ and $\text{ord}(h)$; a subgroup of $G \times H$ need **not** be of the form $G_1 \times H_1$ with $G_1 \leq G$ and $H_1 \leq H$; an abelian subgroup $H \leq G$ need **not** be contained in $Z(G)$; if N and G/N are nilpotent, G need **not** be nilpotent (as opposed to solvable groups!); if a prime power p^n divides $|G|$, then G need **not** have an element of order p^n (but it has one of order p by Cauchy's theorem); if m divides $|G|$, then there need **not** exist a subgroup of G of order m (but it must exist if G is abelian!) ...

RELATED PROBLEMS

1. (April 77 #5) (a) Show the alternating group A_n is normal in S_n.
   (b) Show A_n is generated by all 3-cycles $(12k)$ for $k = 3, 4, \ldots, n$.
   (c) Show any normal subgroup of A_n which contains a 3-cycle must be all of A_n.

2. (May 78 #1) Name a nonabelian simple group.

3. (May 78 #2) If a finite p-group G acts linearly on a finite-dimensional vector space over $\mathbb{F}_p$, show G has a nonzero fixed point.

4. (Jan 79 #8) Do the elements of finite order in a group always form a subgroup?

5. (March 83 #3) Show that S_8 contains a subgroup H of order 15, but S_n for $n < 8$ doesn't.

6. (Feb 84 #7) If H, K are subgroups of G with $Ha = Kb$ for some a, b in G, prove $H = K$. What can you say if $aH = Kb$?

7. (Sep 86 #6) For what n is $S_n \longrightarrow \text{Aut}(S_n)$ (via $g \longrightarrow \kappa_g$ conjugation by g) a monomorphism?

8. (Jan 87 #2) If G is infinite but some nontrivial element $x \neq 1$ has only a finite number of conjugates, show G is not simple.

9. (Aug 89 #1) State the class equation for a finite group, and use it to show $Z(G) > 1$ for a nontrivial p-group G, then prove G is nilpotent.

10. (Jan 89 #2) (a) If G has a normal subgroup N with $G/N = \mathbb{Z}$, show for all $n \neq 0$ there is a normal subgroup N_n with $G/N_n = \mathbb{Z}_n$.
(b) If all proper factor groups G/N of G are finite, must G be finite?

11. (May 89 #5) If H, K are subgroups of G show G is a disjoint union of double cosets HgK.

12. (May 90 #1) If G has no nontrivial automorphisms, prove it has order 1 or 2.

13. (May 92 #3) Prove $V = \{1, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of the symmetric group S_4 on 4 symbols, and that $S_4/V \cong S_3$.

14. (May 92 #5) Use the subgroup structure of the cyclic group of order $n \geq 1$ to show that $n = \sum_{d|n} \phi(d)$, where the Euler ϕ-function $\phi(n)$ is the number of integers $1 \leq k \leq n$ which are relatively prime to n.

15. (Sep 93 #7) A well-known puzzle has tiles numbered 1 to 15 in 4 rows of 4 each, with the (4,4) square empty. An allowable move consists of sliding a tile adjacent to the empty square horizontally or vertically into the empty square. If a sequence of moves ends up with the empty square back at (4,4), prove the resulting permutation π of the numbers 1 to 15 belongs to A_{15}.

16. (Jan 94 #6) (a) Explain why the inner automorphism group of the alternating group A_n is isomorphic to A_n for $n \geq 4$.
(b) Prove that for $n \geq 3$, A_n has outer (:= not inner) automorphisms.

17. (Aug 95 #1) Let G be a finite group of permutations of a finite set X. For $x \in X$ let $G_x = \text{Stab}(x) = \{g \in G \mid gx = x\}$. If $|X| = [G : G_x]$ for some $x \in X$, show the same holds for *all* $x \in X$.

18. (Jan 95 #5) Give definitions of the terms "maximal subgroup" and "minimal subgroup" ; it is not assumed that you have seen these terms previously. Then from your definitions, prove the following facts:
(a) A minimal subgroup must be cyclic of prime order.
(b) If a subgroup has prime index, it is a maximal subgroup.
(c) If a subgroup is both maximal and normal, it has prime index.
(d) A subgroup of an abelian group is maximal if and only if it has prime index.
(e) Find all maximal and minimal subgroups of $\mathbb{Z}$.

19. (Aug 95 #7) Find the order of the group $GL_n(\mathbb{Z}_p)$ and describe one of its p-Sylow subgroups.

20. (Aug 96 #1) A *Hall subgroup* H of a finite group G is a subgroup whose order and index are relatively prime. Use isomorphism theorems to prove that if N is a normal subgroup of G and H is a Hall subgroup of G, then HN/N is a Hall subgroup of G/N, and $H \cap N$ is a Hall subgroup of N.

21. (Aug 97 #2) (a) Prove that if G is a finite group with exactly two conjugacy classes of elements, then $|G| = 2$.
(b) If G has exactly three conjugacy classes of elements, show that $|G|$ involves at most two primes.

(c) There are, in fact, only two finite groups with exactly three conjugacy classes of elements. Can you guess which ones they are?

22. (Aug 98 #2) Let $GL_2(p)$ for a prime p denote the group of invertible 2×2 matrices over the finite field $\mathbb{F}_p$ of p elements.
(a) Find the order n of the group $GL_2(p)$.
(b) For λ in $\mathbb{F}_p$, and $B := \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, find the order m of the subgroup

$$G_\lambda := \{A \in GL_2(p) \mid ABA^{-1} = B\}.$$

(c) Find how many 2×2 matrices over $\mathbb{F}_p$ are similar to the matrix B. (*Hint:* express it in terms of m and n.)

23. (Aug 99 #2) Let G be a finite p-group for a prime p having a unique subgroup G_p of order p. (The quaternion group is such a group, with $p = 2$ and $G_2 = \{1, -1\}$.)
(a) Show that G_p is invariant under all endomorphisms of G, $f(G_p) \subseteq G_p$ for all homomorphisms $f : G \longrightarrow G$.
(b) Show that G_p "needs room" in order to act: whenever G acts on a finite set S of size $|S| < |G|$, the subgroup G_p acts trivially. Conclude that G can only act faithfully on sets of size $\geq |G|$.

24. (Jan 00 #4) (a) If G is a group containing a cyclic normal subgroup N, *show* that $gn = ng$ for all n in N and all g in the commutator subgroup of G.
(b) Suppose that N_1, N_2, N_3 are three normal subgroups of a group G with the properties that for distinct i, j always $N_i \cap N_j = 1$, $N_i N_j = G$. *Show* that all three subgroups N_i are isomorphic, and that G is abelian. Give an *example* of such an abelian group of order 4.

25. (Aug 01 #1) If $\phi : G_1 \to G_2$ is a homomorphism of groups, and $N_1 \lhd G_1, N_2 \lhd G_2$ are two normal subgroups, show that the map $\overline{\phi}$ given on cosets by $\overline{\phi}(xN_1) = \phi(x)N_2$ is a well-defined homomorphism $\phi : G_1/N_1 \to G_2/N_2$ of quotient groups *if and only if* the original homomorphism satisfies $\phi(N_1) \subseteq N_2$.

26. (Aug 02 #3) Let G be a group. Show that if, for any three elements $x, y, z \in G$, at least two of them commute, then G itself is abelian. (*Hint.* Use centralizers.)

27. (Aug 02 #4) Show that a finite group is noncommutative if and only if it has an irreducible complex representation of dimension > 1.

28. (Aug 02 #7) Let p be a prime > 2.
(a) Show that in the symmetric group S_p, any two elements of order p are conjugate.
(b) Exhibit two nonconjugate elements of order p in the symmetric group S_{p^2}.
(c) Are there nonconjugate elements of order p in the group $GL_2(\mathbb{C})$?
(d) Can you find an element of order p in $GL_2(\mathbb{R})$?

29. (Jan 04 #1) Show that the group G_1 of all real numbers for addition is isomorphic to the group G_2 of all positive real numbers for multiplication. Furthermore, show that the group H_1 of all rational numbers is **not** isomorphic to the group H_2 of all positive rational numbers for multiplication.

30. (Jan 04 #2) Let G be a group such that there exists a surjective group homomorphism $G \to \mathbb{Z}$. Prove that for any subgroup of finite index $H \leq G$ there also exists a surjective group homomorphism $H \to \mathbb{Z}$.

31. (Jan 04 #5) Let $G = \{g_1, \ldots, g_n\}$ be a finite abelian group. Show that the product $P := g_1 \ldots g_n$ is of order 1 or 2.

32. (Jan 04 #8) Let S be a finite set acted upon by a finite group G. Denote by $\mathbb{C}(S) = \{f : S \to \mathbb{C}\}$ the space of functions on S.
(a) Show that the map $G \times \mathbb{C}(S) \to \mathbb{C}(S)$, $(x, f) \mapsto xf$, defines a G-action on $\mathbb{C}(S)$. Here $xf \in \mathbb{C}(S)$ is defined by $xf(s) = f(x^{-1}s)$.
(b) Show that the dimension of the subspace of G-fixed points in $\mathbb{C}(S)$ is equal to the number of G-orbits in S.

33. (Aug 04 #1) Assume that the group G is a direct product of two finite subgroups A and B, $G = A \times B$, and that $|A|$, $|B|$ are relatively prime. Show that $H = (H \cap A) \times (H \cap B)$ for any subgroup H of G.

34. (Jan 05 #1) Write down the class equation for the dihedral group D_{20} of order 20.
No proof required but you should identify the terms in your equation.

35. (Aug 05 #2) Let G be finitely generated group.
(a) If H is a finite group, show that there exist only finitely many group homomorphisms from G to H.
(b) (6 points) If n is a given natural number, show that there exist only finitely many normal subgroups N of G with $[G : N] = n$.

36. (Aug 06 # 2) Let G be a finite group wherein any two conjugate elements commute. Prove that G is solvable. (More is true: G actually has to be nilpotent; that is, however, a little harder to show.) There is partial credit for proving that G is not simple unless it is abelian.

37. (Jan 08 #1) Show that a group G will have outer automorphisms (automorphisms which are not inner) if it can be properly imbedded as a normal subgroup $G \triangleleft G'$ of a group in such a way that $G \cdot \text{Centralizer}_{G'}(G) \neq G'$.
(b) Show that A_n has outer automorphisms whenever $n \geq 4$.
(c) Explain the mantra "Every automorphism of G is inner, somewhere."

38. (Aug 08 #7) The goal of this problem is to prove that all automorphisms φ of S_5 are inner.
a. Given that the transpositions (i, j) $(i < j)$ generate S_n, *prove* that the adjacent transpositions $\tau_i := (i, i+1) \in S_n$ for $1 \leq i \leq n-1$ generate S_n.
b. Prove that all automorphisms of S_n leave A_n invariant, $\varphi(A_n) = A_n$.
c. Prove that the elements of order 2 in S_5 are precisely all single and double transpositions (i, j) and $(i, j)(k, \ell)$ for distinct i, j, k, ℓ, then use part (b) to show that $\varphi(\tau_i)$ is a single transposition for every automorphism $\varphi \in Aut(S_5)$.
d. Prove that every automorphism $\varphi \in Aut(S_5)$ is an inner automorphism. [Hint: count possibilities for $\varphi(\tau_i)$ to get an upper bound on the number of automorphisms of S_5].

39. (Aug 09 #2) Let G be a finite group and let H and K be subgroups of G. For each $x \in G$ define $HxK = \{hxk : h \in H, k \in K\}$.

(a) Prove that for any $x, y \in G$ either $HxK = HyK$ or $HxK \cap HyK = \emptyset$.
(b) Prove that $|HxK| = |H||K|/|H \cap xKx^{-1}|$. **Hint:** Use group actions: either a suitable action of $H \times K$ on G or a suitable action of H on G/K.

40. (Aug 09 # 8) Let F be a field. Prove that the additive and multiplicative groups of F cannot be isomorphic. **Hint:** Look at the orders of elements in both groups.

41. (Aug 10 #2) Let G be a group. A subgroup H of G will be called *essential* if $H \cap K \neq \{1\}$ for every non-trivial subgroup K of G.
(a) Let p be a prime and $k \geq 2$. Prove that the group $\mathbb{Z}/p^k\mathbb{Z}$ has a proper essential subgroup.
(b) Assume that H_1 is an essential subgroup of G_1 and H_2 is an essential subgroup of G_2. Prove that $H_1 \times H_2$ is an essential subgroup of $G_1 \times G_2$.
(c) Let G be a finite abelian group. Prove that G does not have a proper essential subgroup if and only if G is a direct product of groups of prime order.

42. (Aug 11 # 2) The following question concerns symmetric groups. You can assume as given the fact that any permutation in S_n can be written (uniquely up to order) as a (commuting) product of disjoint cycles (of varying lengths). Otherwise, your argument should be self-contained.
(a) For $n \geq 2$, show that the symmetric group S_n is generated by the transpositions (i, j), $1 \leq i < j \leq n$.
(b) For $n \geq 3$, show that the alternating group A_n is generated by the 3-cycles (1, 2, i), $2 < i \leq n$.
(c) Let H be a subgroup of a group G of index n. Show that G has a normal subgroup N which is contained in H and which has index $\leq n!$.

43. (Aug 11 # 6a) Suppose that $G = C_p \times \ldots \times C_p$ is a direct product of n copies of the cyclic group C_p of order p. How many subgroups does G have of order p? How many does it have of order p^{n-1}? Explain.

44. (Jan 12 # 2) Let G be a subgroup of the symmetric group S_n for some integer $n > 1$. Assume that G acts transitively on $\mathbf{n} := \{1, 2, \ldots, n\}$, that is, for any $i, j \in \mathbf{n}$ there exists $g \in G$ s.t. $g(i) = j$.
A partition of $\mathbf{n}$ is a decomposition $\mathbf{n} = X_1 \cup \ldots \cup X_m$ into a disjoint union of nonempty subsets. There are two trivial partitions: $\mathbf{n} = \mathbf{n}$ and $\mathbf{n} = X_1 \cup \ldots \cup X_n$ (so each X_i has just one element). Otherwise the partition is said to be nontrivial. The group G is called **imprimitive** if there is a nontrivial partition $\mathbf{n} = X_1 \cup \ldots \cup X_m$ such that, for $g \in G$ and $1 \leq i \leq m$, $g(X_i) = X_j$ for some j. (That is, G permutes the partition members among themselves.) The set $\{X_i\}$ is called a system of imprimitivity for the action of G on $\mathbf{n}$. The group G is called **primitive** if it is not imprimitive.
(a) Let $n = 6$ and consider the cyclic subgroup $G := \langle(1, 2, 3, 4, 5, 6)\rangle$ of S_6. There are two non-trivial systems of imprimitivity for the action of G on $\mathbf{n}$. Find them.
(b) Prove that if $X_1 \cup \ldots \cup X_m$ is a system of imprimitivity for the action of G on $\mathbf{n}$, then all subsets X_i have the same size n/m.
(c) G is said to be doubly transitive if given elements $a, b, c, d \in \mathbf{n}$, with $a \neq b$ and $c \neq d$, there exists $g \in G$ such that $g(a) = c$ and $g(b) = d$. Show that a doubly transitive group G

is primitive.
(d) Show that if $n \geq 3$, the alternating subgroup $G = A_n$ of S_n is primitive.

45. (Aug 12 #1) For a positive integer n, denote by S_n the symmetric group on $\{1, 2, \ldots, n\}$. Let $p > 2$ be a prime number.

    (a) (2 pts) Give an example of a non-cyclic group of order $2p$.

    (b) (5 pts) Find the smallest n for which S_n contains a cyclic subgroup of order $2p$.

    (c) (7 pts) Find the smallest n for which S_n contains some subgroup of order $2p$.

    In both (b) and (c), if n is your answer, explain clearly why S_n contains a desired subgroup and why S_m for $m < n$ does not contain such subgroup.

46. (Jan 13 #1) Let p be a prime and let S_{2p} denote the symmetric group on $2p$ elements.

    (a) (2 pts) Find the order of a p-Sylow subgroup of S_{2p}.

    (b) (5 pts) Describe explicitly a p-Sylow subgroup of S_{2p} (providing a generating set counts as explicit description, but make sure to prove that your subgroup is indeed p-Sylow).

    (c) (2 pts) Consider the set of elements of order p in S_{2p} – clearly, it is a union of conjugacy classes. How many conjugacy classes does it consist of?

    (d) (5 pts) Now consider the set of elements of order p in the alternating group A_{2p}. How many conjugacy classes (of A_{2p}) does it consist of? Make sure to justify your answer.

    Hint: Distinguish between the cases $p = 2$ and $p > 2$.

47. (Aug 13 #1) Let p be an odd prime and G a nonabelian group of order p^3.

    (a) (4 points) Prove that $|Z(G)| = p$

    (b) (4 points) Prove that $Z(G) = [G, G]$.

48. (Aug 13 #3) If G is a group, then there is a natural action of Σ_n on $G^{\times n}$ given by permuting the factors. Define the wreath product $G \wr \Sigma_n$ to be

$$G \wr \Sigma_n = G^n \rtimes \Sigma_n$$

    using this action of Σ_n on G^n.

    (a) (3 points) If X is a G-set, show that X^n is naturally a $G \wr \Sigma_n$ set by combining two actions: G^n on X^n via

$$(g_1, \ldots, g_n) \cdot (x_1, \ldots, x_n) = (g_1 x_1, \ldots, g_n x_n)$$

    for $(g_1, \ldots, g_n) \in G^n$ and $(x_1, \ldots, x_n) \in X^n$, and
    Σ_n on X^n via

$$\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}),$$

    where $\sigma \in \Sigma_n$.

    (b) Show that $\Sigma_n \wr \Sigma_m$ embeds into Σ_{nm}.

(c) Identify $\Sigma_2 \wr \Sigma_2$ with a more familiar group

(d) Determine the order of $G \wr \Sigma_n$ as a function of the orders of G and n

(e) Bonus: Determine (no proof needed) the p-Sylow subgroup of $\Sigma_{p^{k+1}}$ as a function of k. Provide no more than a sentence of justification.

49. (Jan 14 #8) Use the semidirect product constructions to classify the groups of order 44. (Hint: start by analyzing Sylow subgroup structures.)

50. (Aug 14 #1) Let G be a finite nilpotent group, Z(G) its center and p a prime number. Prove that p divides $|G|$ if and only if p divides $|Z(G)|$.

51. (Aug 14 #3) Let p be a a prime number.
(a) Determine the order of the automorphism group of $\mathbb{Z}_p \times \mathbb{Z}_p$.
(b) Prove that there exists a non-abelian group of order p^3.

52. (Aug 14 #6) (a) Compute the order of the group G of rigid motions of a regular octahedron O.
(b) The group G acts on the set of vertices of O. Describe the stabilizer of a vertex of O.

53. (Aug 15 #3) (a) Let G be a group of order $2n$, where n is odd and $n > 1$. Prove that G cannot be simple.
(Hint: consider elements of order 2 in the regular representation of G in S_{2n}.)
(b) Let $G = \mathbb{Z}_n^*$ denote the group of units in $\mathbb{Z}_n$. Find all integers n such that $x^2 = 1$ for all $x \in G$.

54. (Jan 16 #2) Let G be an infinite group and let H be a subgroup of finite index. Prove that there exists a subgroup K of H such that K has finite index in G and such that K is normal in G.

55. (Jan 16 #4) Let $G = S_n$ be the symmetric group on n elements, and let $\sigma = (123\ldots n)$ be an n-cycle. Let K be the cyclic subgroup generated by σ. Prove that the order of the normalizer of K, i.e., the order of the subgroup $H = \{x \in S_n \mid x^{-1}\sigma x \in K\}$, is exactly $n \cdot \phi(n)$, where $\phi(n)$ is the Euler ϕ-function. (Recall that $\phi(n)$ is the number of positive integers less than n and relatively prime to n.)

56. (Aug 16 #2) What is the smallest integer m such that there is a group of order m with no nontrivial normal p-subgroup for any prime p?

57. (Jan 17 #4) We call a group G polycyclic if it contains a series of subgroups $\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$ such that G_i/G_{i-1} is a (possibly infinite) cyclic group.
(a) Show that a finite group is polycyclic if and only if it is solvable.
(b) Show that $\mathbb{Q}$ is an example of an abelian group which is not polycyclic.

58. (Jan 17 #5) Given a finite group G and two subgroups H, K, the double cosets of H and K are the sets of the form HgK for some $g \in G$.
(a) Show that any two double cosets must be equal or disjoint.
(b) Show that the size of any double coset must divide the product of the orders $|H| \cdot |K|$.
(c) Find an example of a double coset whose size does not divide the order $|G|$.

59. (Jan 17 #6)
(a) Find the smallest integer n such that S_n has a subgroup of order 10, but S_k for $k < n$ does not.
(b) Find the smallest integer m such that S_m has an element of order 10, but S_k for $k < m$ does not.

60. (Aug 17 #1) Denote by D_{2n} the dihedral group of order $2n$, $n = 1$ being admitted. For which natural numbers m and n is D_{4nm} isomorphic to the direct product $D_{2m} \times D_{2n}$?

61. (Jan 18, #1) Classify, up to isomorphism, all finite groups of order $2p$, where p is a prime number.

1.2 Applications of the Sylow Theorems

KNOW ALL PARTS TO THE SYLOW THEOREM: If $|G| = p^e m$ for a prime p and a natural number m with $(p, m) = 1$, a *Sylow p-subgroup* of G is any subgroup P with $|P| = p^e$, i.e. a p-subgroup of the maximal possible order.
(i) (**Existence**) If p is a prime number and p^α divides the order of G then G has a subgroup of order p^α (in particular, Sylow p-subgroups exist).
(ii) (**Inclusion**) Any p-subgroup of a finite group G is contained in a Sylow p-subgroup of G (so the Sylow p-subgroups of G can also be characterized as the *maximal* p-subgroups of G).
(iii) (**Conjugacy**) Any two Sylow p-subgroups of G are conjugate.
(iv) (**Number**) The number n_p of them is congruent to 1 mod p, and divides m (the number is exactly the index of the normalizer of any particular P, $n_p = [G : N_G(P)]$).

BASIC FACT: Any conjugate of a Sylow subgroup is Sylow, so *if for some p there is only one Sylow p-subgroup, it must be a normal subgroup* (proper unless G itself is a p-group, $|G| = p^e$, in which case it is nilpotent, hence solvable, hence not simple, unless $|G| = p$).

KNOW THE 3 PRINCIPAL METHODS OF PROVING THAT A GROUP IS NOT SIMPLE (which by induction can often be improved to showing that the group is SOLVABLE):
1. **Simple Sylow Count**: Use (iv) to show that the number of Sylow p-subgroups is 1. Examples: $|G| = 1776$ [Sep 83 #1], 1989 [Jan 89 #1], 1995 [Jan 95 #1; show G solvable], 1001 [Aug 95 #2; show G abelian, cyclic], 200 [Aug 88 #4 ;1985 #1a]; $n = 20, 28, 44, 52$; $n = p^e m$ for $p > m$.
2. **Small Index**: Show that $|G|$ does not divide $n_p!$ for some prime p, eg p^e doesn't divide $(m-1)!$ (Reason: G acts transitively on the set $\mathcal{P}$ of Sylow p-subgroups by conjugation, so by simplicity either (i) G embeds faithfully in $Sym(\mathcal{P})$ of size $n_p!$, so $|G| \mid n_p! \mid m!$, or (ii) G is mapped onto the identity, in which case by transitivity there would be only one P, contrary to the Basic Fact). Examples: $|G| = 24, 36, 48; 72$ [Jan 87 #1, Sep 84 #1] .
3. **Element Count**: Use (iv) to get estimates on $n_p > 1$ for the relevant p's, and count how many elements there are of order p^k for the various k and p (crucial: two subgroups of prime order p can overlap only in one element; the answer is not so simple for Sylow subgroups of higher order p^k), and show the number of elements would be $> |G|$. Examples: $|G| = 30$, 56.

KNOW THE FOLLOWING CHARACTERIZATION OF FINITE NILPOTENT GROUPS:
G is nilpotent iff all its Sylow subgroups are normal iff G is the direct product of its Sylow subgroups.

RELATED PROBLEMS

1. (Nov 77 #7) Must a group of order 70 be abelian? Solvable? Can you say anything about its normal subgroups?

2. (a) (January 81 #5, Sep 78 #3) If G of order 60 has exactly 4 elements of order 5, there is a proper normal subgroup.
(b)If G of order 60 has more than 4 elements of order 5, then G is simple (and hence isomorphic to A_5).

3. (January 82 #VIIa, May 89 #8, Sep 93 #3) If a normal subgroup H of G contains a Sylow subgroup P of G, then $G = HN_G(P)$.

4. (Jan 82 #VIIb,c) The *Frattini subgroup* F of G is defined to be the intersection of all maximal subgroups of G. Show
(a) F is normal in G,
(b) if G is finitely generated then F is inessential ($G = FH \Longrightarrow G = H$),
(c) if F contains a p-Sylow subgroup of G then that subgroup is normal.
Comments: Do (b) first for finite groups. Then prove for finitely generated G that every proper subgroup of G is contained in a maximal subgroup (mimic the standard proof for commutative rings with 1 that proper ideals are contained in maximal ideals). In (c) we assume that G is finite.

5. A member g of a group G is called a *nongenerator* of G if whenever G is generated by a subset containing g, it is also generated by the subset with g removed. It is a fact that the set of all nongenerators of G forms a subgroup, the *Frattini subgroup* of G. If F is the Frattini subgroup of a finite p-group G (p a prime), show that $g \in F$ iff g is in every subgroup of index p of G. (You may use the fact that if H is a proper subgroup of G, then H is a proper subgroup of its normalizer $N_G(H)$). Conclude that G/F is an abelian group of exponent p.

6. (Sep 82 #6) If G is nonabelian of order 21, show it is generated by elements s, t with $s^7 = t^3 = 1, t^{-1}st = s^2$.

7. (Sep 86 #2) Find ALL groups of order 99.

8. (Fall 87 #1) If G of order 160 has two distinct subgroups of order 80, then G has a normal subgroup of order 5.

9. (May 90 #2) A group of order 441 is solvable.

10. (May 91 #4b) If G is a group of order 231, show the 11-Sylow subgroup H of G is normal in G and lies in the center of G. (*Hint:* Let G act on H by conjugation.)

11. (Jan 92 #4) If a finite group G has a normal p-Sylow subgroup P, then $\phi(P) \subseteq P$ for every endomorphism ϕ of G.

12. (Jan 94 #4) Let $f : G \longrightarrow H$ be a surjective homomorphism of finite groups, and let p be a prime.
(a) Prove that if P is a p-Sylow subgroup of G, then $f(P)$ is a p-Sylow subgroup of H.
(b) Prove that every p-Sylow subgroup of H has the form $f(P)$ for some p-Sylow subgroup P of G.

13. (Aug 94 #1) Let P be a p-Sylow subgroup of a finite group G, p a prime dividing the order of G.
(a) Prove that P consists of all the p-torsion elements of the normalizer $N_G(P)$, that is, all elements of $N_G(P)$ whose order is a power of p. (*Hint:* apply Sylow to $N_G(P)$.)
(b) Prove that P is a characteristic subgroup of $N_G(P)$, that is, is invariant under all automorphisms of $N_G(P)$.
(c) Prove that $N_G(N_G(P)) = N_G(P)$.

14. (Aug 96 #8) Give an example of two finite groups whose Sylow subgroups are isomorphic for each prime, but which are not themselves isomorphic.

15. (Jan 97 #6) Let P be a p-Sylow subgroup of a finite group G. Prove that if H is a subgroup of G, then for some $g \in G$, $H \cap gPg^{-1}$ is a p-Sylow subgroup of H.

16. (Jan 98 #1a) What can you say about groups of the following orders n? (Give reasons, making free use of any theorems you know.)
(a) $n = 2^4 + 1$.
(b) $n = 2^3 + 1$.

17. (Aug 98 #1ab) Let G be a finite group of order $3 \cdot 5 \cdot 17$. Show that the Sylow 17-subgroup is normal. If there exists an element of order 15 in G, show that the Sylow 3- and 5-subgroups are also normal. (*Hint:* show they are properly contained in their normalizers.)

18. If G and its normal subgroup N have the same power of p, then all p-Sylow subgroups of G live in N; if one is normal in N, then it is the unique p-Sylow subgroup of G.

19. (August 98 #1c) If all Sylow subgroups of a finite group G are normal and abelian, show that G itself is abelian.

20. (Aug 99 #1) Show that if $G \supseteq M \supseteq N_G(P)$ for a p-Sylow subgroup P of a finite group G, then $[G : M] \equiv 1 \pmod{p}$.

21. (Jan 00 #5) Let G be a finite group such that every element commutes with its conjugates (for any $g, h \in G$ the elements h and ghg^{-1} commute).
(a) Show that any Sylow subgroup of such a G is normal. [Hard!]
(b) *Explain* why the group of quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$ is such a group G.

22. (Aug 01 #2) Show that if p is a prime and H is a subgroup of G, then the number of distinct p-Sylow subgroups of H is less than or equal to the number of distinct p-Sylow subgroups of G.

23. (Aug 03 #7) Let G be a finite group of order n. Suppose that for every d dividing n, the equation $x^d = 1$ has at most d solutions in G. Show that:
(a) For each prime p, the Sylow p-subgroup of G is unique, and thus is normal.
(b) The Sylow p-subgroup of G is cyclic.
(c) Use (a) and (b) to show that G is cyclic.

24. (Aug 04 #2) Let G be a group of order 56, and let P_p for $p \in \{2, 7\}$ be a Sylow p-subgroup of G.
(a) Show that P_2 or P_7 is normal in G.
(b) Give an example of a group G with $|G| = 56$ where P_2 is not normal.
(c) Show that there exists a group G of order 56 with a non-normal P_7. You can either do this by exhibiting a concrete example with this property or by describing how to construct such a group. In the latter case you have to justify why your approach works but you needn't give all details of the construction.

25. (Jan 05 #2) Consider the following two statements:
(a) Any group of order 455 is abelian.
(b) Any group of order 455 is solvable but there exist non-abelian groups of order 455.
Decide which of the two statements is true (2 points) and prove it.

26. (Aug 05 #1) Let G be a group of order 60 which acts transitively on a set S with 20 elements. Prove that there exist two elements $x, y \in S$ with $x \neq y$ and equal stabilizers $G_x = G_y$.

27. (Jan 06 #3) If a prime p divides the order of a finite nonabelian simple group G, show that $|G| < n_p!$ where n_p is the number of distinct p-Sylow subgroups of G.

28. (Aug 06 #1) Prove that there is no simple group of order $2 \times 3^3 \times 5^2$.

29. (Aug 06 #3) Show that any nilpotent group G of order 900 is abelian.

30. (Aug 08 #6) Let G be a group of order pqr where p, q, r are prime numbers with $(i) p > q > r$, $(ii) \gcd(q, p-1) = \gcd(r, q-1) = \gcd(r, p-1) = 1$.
a. Prove that G has a normal subgroup P of order p.
b. Prove that G has a subgroup Q of order q which commutes with P, so that $P \times Q$ is a subgroup of G of order pq.
c. Prove that Q is normal, so $P \times Q$ is a normal subgroup of G.
d. Prove that G has a subgroup R of order r which commutes with $P \times Q$, so that $P \times Q \times R$ is a subgroup of G. Conclude that G is cyclic.

31. (Jan 09 #1) Let G be a group of order $660 = 11 \cdot 60$, and let P be a Sylow 11-subgroup of G. Assume that $C_G(P) = P$.
(a) Prove that $|N_G(P)| = 55$.
(b) Let H be a normal subgroup of G. Prove that either $P \subseteq H$ or $|H| \equiv 1 \bmod 11$. **Hint:** Consider the conjugation action of P on H.

32. (Aug 09 #1) Let G be a group of order 56 which does NOT have a normal subgroup of order 8.

(a) Prove that G has a normal subgroup of order 7.
(b) Prove that G has a subgroup of order 14.
(c) Prove that G has a normal subgroup of order 14.
Remark: Of course, you may omit (b) if you correctly answered (c).

33. (Aug 10 # 1) Let p be prime. Let G be a finite group, K a normal subgroup of G, and assume that $|G/K|$ is divisible by p. Let P be a Sylow p-subgroup of G.
(a) Prove that PK/K is a Sylow p-subgroup of G/K.
(b) Prove that $n_p(G/K)$ divides $n_p(G)$ where $n_p(\cdot)$ denotes the number of Sylow p-subgroups.
(c) prove that $n_p(G/K) = n_p(G)$ if and only if P is normal in PK.

34. (Aug 11 # 7) (a) Let G be a finite simple group of order 168. How many elements of order 7 does G have? Why?
(b) How many conjugacy classes of elements of order 7 does G have? Hint: By looking at Sylow 3-subgroups, show that G has no cyclic subgroup of order 21. Use this to determine the centralizer in G of an element of order 7. . . . .
(c) Assume that you know that $G := GL_3(\mathbb{F}_2)$ is a simple group. Explicitly exhibit two elements of G of order 7 which are not conjugate in G. Explain.

35. (Jan 12 # 1) Let $F = \mathbb{F}_q$ be a finite field, where $q = p^r$ is a power of a prime p. Let $G = GL_n(F)$ be the group of all $n \times n$ invertible matrices with entries in F. Once you pick an ordered basis of $V := F^n$, you may find it useful to identify G with the group of invertible linear operators on V.
(a) Calculate the order of G. Explain your answer carefully and write it in the simplest form as you can.
(b) Determine the order of a Sylow p-subgroup of G, and explicitly exhibit a Sylow p-subgroup U of G.
(c) What is the normalizer in G of the Sylow p-subgroup U that you exhibited in (b)? An answer is sufficient.
(d) How many Sylow p-subgroups of G are there? Explain how your answer in (d) is consistent with Sylow's theorem.

36. (Aug 12 # 2) Let G be a finite group and p a prime divisor of $|G|$. Assume that every element of G of p-power order is contained in a normal p-subgroup of G. Show that G has only one Sylow p-subgroup.

37. (Aug 16 #4) Fix a group G.
(a) Show that if N is a normal Sylow p-subgroup of G and H a subgroup of order not divisible by p, then HN is a subgroup of G isomorphic to a semi-direct product $N \rtimes H$.
(b) Consider a group G of order 255. Show that G is cyclic.

38. (Aug 17 #2) Let G be a group of order $16 \cdot 11 \cdot 13 \cdot 17$. Assume that G has a normal nonabelian Sylow 2-subgroup. Show that the center of G is nontrivial.
Remark: The claim remains true if G has an abelian normal Sylow 2-subgroup but then it is a bit harder to prove.

1.3 Abelian Groups

KNOW BASIC DEFINITIONS: Free abelian group, rank, torsion, direct sum, elementary divisors, invariant factors.

KNOW THE FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUPS:
Every finitely generated abelian group A is of the form $A = T(A) \oplus F(A)$, where $T(A)$ is the (finite) torsion subgroup of A and $F(A)$ is a free abelian group of finite rank $n \in \mathbb{N}_0$ (i.e. $F(A)$ is isomorphic to $\mathbb{Z}^n$), with n, the "Betti number" of A, uniquely determined by A.
Regarding $T(A)$ (which is of course A if A is finite):
Elementary Divisor Form (longest decomposition into cyclics)
$T(A) = \mathbb{Z}_{p_1^{f_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{f_s}}$ where the p_i's are (not necessarily distinct) prime numbers, and the number of summands of type $\mathbb{Z}_{p^f}$ (the elementary divisors) are invariants of $T(A)$ and A; $T(A)$ is cyclic iff all elementary divisors have distinct primes.
Invariant Factor Form (shortest decomposition into cyclics)
$T(A) = \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_l}$ for $d_1 \mid d_2 \mid \cdots \mid d_l$ where the invariant factors $d_i \in \mathbb{N}$ with $d_i > 1$ are invariants of $T(A)$ and of A; $T(A)$ is cyclic iff $l = 1$.

KNOW HOW TO COUNT: the number of non-isomorphic finite abelian groups of order $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where this time the p_i's are distinct primes, is $\mathcal{P}(e_1)\mathcal{P}(e_2)\cdots\mathcal{P}(e_r)$ for $\mathcal{P}(e)$ = number of partitions of the exponent e (the number of ways of writing $e = f_1 + \cdots + f_s$ for $1 \le f_1 \le \cdots \le f_s$).

KNOW HOW TO DECOMPOSE:
(I) Write $A = F/K$ for F free on N generators $\{x_1, \ldots, x_N\}$ with M relations $B\vec{x} = \vec{0}$ (ie. $b_{i1}x_1 + \cdots + b_{iN}x_N = 0$ for $i = 1, 2, \ldots, M$).
(II) Rewrite equations $B \longrightarrow UB$ for elementary U (elementary row operations), change basis of free module F into $\{y_1, \ldots, y_N\}$ by $B \longrightarrow BV$ for elementary V (elementary column operations), until reach "diagonal form" $\mathrm{diag}(d_1, \ldots, d_n)$ with $n \le \max\{M, N\}$, $d_1, \ldots, d_n \in \mathbb{N}$ and $d_1 \mid d_2 \mid \ldots \mid d_n$. Set $d_i := 0$ for $n < i \le N$.
(III) Then $F = \oplus\mathbb{Z}y_i$, $K = \oplus\mathbb{Z}d_i y_i$, $A = F/K \cong \oplus\mathbb{Z}/d_i\mathbb{Z} = \oplus_{d_i \neq 1}\mathbb{Z}_{d_i}$.
(Figuratively speaking: reduce the matrix to the diagonal form using elementary row and column operations.)

KNOW HOW TO GO BACK AND FORTH BETWEEN INVARIANT FACTORS AND ELEMENTARY DIVISORS: InvFac $\longrightarrow$ ElDiv by factoring each $d_i = \prod p_{ij}^{e_{ij}}$, ElDiv $\longrightarrow$ InvFac by $d_N = \prod p_i^{\text{highest } e_i}$, $d_{N-1} = \prod p_i^{\text{next highest } e_i}$, etc.

RELATED PROBLEMS

1. Describe (up to isomorphism) all abelian groups of order: [May 91 #4a] 4851; [85 #1c] 2334; [Aug 88 #4] 200; [Jan 87 #1] 72; [Feb 84 #1] 1984; [Sep 80 #1] 80; [May 80 #1] 375.
2. How many non-isomorphic abelian groups are there of order: [Sep 83 #1] 1776, [Jan 98 #2a] 360.

3. (April 77 #3) Use the Fundamental Theorem of Finite Abelian Groups to show the multiplicative group of the ring $\mathbb{Z}_{p^n}$ for prime p, $n > 1$ has a subgroup of order p.

4. (May 78 #6) Give an example of a torsion-free abelian group which is not free. Can you give an example which is finitely generated?

5. (Mar 83 #6) Show a finite abelian group is cyclic iff it has no subgroup isomorphic to $B \oplus B$ for $B \neq 0$.

6. (Aug 89 #6) Find the structure of all abelian groups generated by 3 elements a, b, c satisfying relations $-4a + 2b + 6c = 0,\ -6a + 2b + 6c = 0,\ 7a + 4b + 15c = 0$.

7. (Jan 92 #1) Show that an infinite abelian group is cyclic iff every nonzero subgroup has finite index.

8. (Aug 94 #2) If G is a finite abelian group of order n, show that G has a subgroup of order d for each divisor d of n. Show that this need not be true if G is not abelian.

9. (Aug 95 #3) Find the order of the abelian group generated by x, y, z subject to the relations $4x - 2y + 4z = 0,\ 7x - 8y + z = 0,\ 8x + y + 13z = 0$.

10. (Aug 96 #2) Determine all pairs of positive integers a, b with $a \leq b$ such that $\mathbb{Z}_a \times \mathbb{Z}_b$ is isomorphic to $\mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{20}$.

11. (Jan 97 #2) Let G be a finite abelian group of order k and n an integer. Show that if k_n is the number of solutions of $g^n = 1$ in G, and $k^{(n)}$ is the number of n-th powers in G, then $k = k_n\, k^{(n)}$.

12. (Jan 98 #2) Take the free abelian group on three generators x, y, z, and divide by the relations $2x + 4y + 5z = 0,\ 6x + 8y + 10z = 0,\ 8x + 12y + 20z = 0$. Write the resulting group as a direct sum of cyclic groups.

13. (Aug 98 #1d) If G is a finite abelian group of order pqr for distinct primes p, q, r, show that G is cyclic.

14. (Aug 98 #3) For an abelian group A, the *dual group* A^* is defined to be $Hom(A, \mathbb{T})$ where the *circle group* or *torus* $\mathbb{T}$ is the multiplicative group of complex numbers of modulus 1 (the unit circle in the complex plane). Here $Hom(A, B)$ denotes the abelian group of homomorphisms of A into B (under $(f+g)(a) = f(a)+g(a)$); you may use the additivity property $Hom(A_1 \oplus A_2, B) \cong Hom(A_1, B) \oplus Hom(A_2, B)$ and the isomorphism property that if $A \cong A', B \cong B'$ then $Hom(A, B) \cong Hom(A', B')$.
(a) Prove that $\mathbb{Z}_n^*$ is cyclic of order n.
(b) Prove that A^* is isomorphic to A for *any* finite abelian group A.

15. (Aug 99 #3) The *exponent* e of a group G is defined as the smallest positive integer k such that $x^k = 1$ for all $x \in G$; for an abelian group, in additive notation this is the smallest k such that $kx = 0$ for all elements. If $n_1, n_2, \ldots, n_r$ are the invariant factors of a finite abelian group A (so $n_r | n_{r-1} | \cdots | n_2 | n_1$), prove that A has exponent $e = n_1$, and has an element of order precisely e. Conclude that A has an element of order m iff m divides the largest invariant factor n_1.

16. (Jan 00 #3)(a) Let A be an abelian group, and let f and g be any two endomorphisms of A (group homomorphisms of A into itself). Let $B := \mathrm{Fix}(fg) = \{a \in A \mid f(g(a)) = a\}$, $C := \mathrm{Fix}(gf) = \{a \in A \mid g(f((a)) = a\}$. *Show* that B and C are isomorphic subgroups of A.
(b) *How many* abelian groups (up to isomorphism) are there of order 1000 which have no elements whose orders are larger than 35?

17. (Aug 01 #3) How many nonisomorphic abelian groups are there of order 325?

18. (Jan 04 #4) Let H be the subgroup of $G := \mathbb{Z} \oplus \mathbb{Z} = \{(m, n) \mid m, n \in \mathbb{Z}\}$ generated by $(1, 2)$ and $(3, 4)$. Identify the quotient group G/H.

19. (Aug 04 #5) Let N be the $\mathbb{Z}$-submodule of $\mathbb{Z}^3$ generated by the column vectors $(2, 2, -2)^t, (-4, -2, 4)^t$ and $(2, 4, 4)^t \in \mathbb{Z}^3$.
(a) Determine the structure of the abelian group $\mathbb{Z}^3/N$.
(b) Determine a basis y_1, y_2, y_3 of $\mathbb{Z}^3$ and natural numbers $d_1 \mid d_2 \mid d_3$ such that d_1y_1, d_2y_2, d_3y_3 is a $\mathbb{Z}$-basis of N.

20. (Aug 05 #8) Let A be a finitely generated abelian group and n a natural number.
(a) Show that A can be generated by n elements if and only if A is a homomorphic image of $\mathbb{Z}^n$.
(b) If B is a subgroup of A, and A can be generated by n elements, prove that also B can be generated by n elements.
(Hint: It is known from the structure theory of modules over PID's that this statement is true for $A = \mathbb{Z}^n$.)
(c) If p is a prime number, prove that *no* subgroup of $\mathbb{Z}^2 \oplus \mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^4}$ is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

21. (Jan 06 #2) Find the number of elements of order precisely p^2 in the group $\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^5}$.

22. (Aug 08 #4) Let G be a finite abelian group, $|G| = n$, and define the exponent of G to be $Exp(G) := \min\{k \in \mathbb{N} \mid g^k = e \textit{ for all } g \in G.\}$.
a. Prove that $Exp(G)$ divides n, and n divides $Exp(G)^j$ for some $j \in \mathbb{N}$.
b. If G, H are finite abelian groups with $Exp(G) = Exp(H)$ and $|G| = |H| = n$ where p^4 does not divide n for any prime p, prove that G and H are isomorphic.
c. State (without proof) results analogous to (a) and (b) which hold for $n \times n$ matrices over an algebraically closed field.

23. (Jan 09 #2) (a) Classify abelian groups of order $72 = 2^3 \cdot 3^2$ up to isomorphism (the answer is sufficient).
(b) Let m and n be positive integers. What is the number of elements in $\mathbb{Z}/n\mathbb{Z}$ whose order divides m?
(c) Let G and H be finite abelian groups, and assume that for any $m \in \mathbb{N}$ the groups G and H have the same number of elements of order m. Prove that G and H are isomorphic.

Chapter 2

Rings

2.1 Basic commutative ring theory

KNOW BASIC DEFINITIONS: (commutative) ring, subring, ring homomorphism, ideal, quotient (or factor) ring, maximal and prime ideal; prime and irreducible elements; (group of) units, associate elements, divisibility, gcd, lcd; field, integral domain, Euclidean domain, PID, UFD, noetherian ring; polynomial ring $R[x]$; rings of fractions.

KNOW THE BASIC LEMMAS: isomorphism theorem(s); I maximal (prime) $\Leftrightarrow$ R/I is a field (integral domain); finite integral domains are fields; Euclidean algorithm (know how to compute the gcd d of a and b as well as coefficients x and y such that $ax + by = d$); universal properties of polynomial rings and rings of fractions.

KNOW BASIC CONSTRUCTIONS: direct products of rings; intersections, sums and products of ideals – recall
$I + J := \{x + y \mid x \in I \text{ and } y \in J\}$
$IJ := \{\sum_{i=1}^{n} x_i y_i \mid n \in \mathbb{N};\ x_i \in I,\ y_i \in J \text{ for all } 1 \leq i \leq n\}$

KNOW EXAMPLES OF EUCLIDEAN DOMAINS: $\mathbb{Z}$; $K[x]$ for a field K; $\mathbb{Z}[\alpha]$ for $\alpha = i$, $\sqrt{-2}$, $\sqrt{2}$, $\sqrt{3}$.

KNOW EXAMPLES OF NON-PID'S: $\mathbb{Z}[x]$; $K[x, y]$ for a field K; $\mathbb{Z}[\alpha]$ for $\alpha = \sqrt{-3}$, $\sqrt{-5}$.

KNOW THE "HIERARCHY": field $\Rightarrow$ Euclidean domain $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ domain

KNOW SOME MORE THEOREMS: Chinese Remainder Theorem; Gauss' Lemma (R UFD $\Rightarrow$ $R[x]$ UFD); Hilbert's Basis Theorem (R noetherian $\Rightarrow$ $R[x]$ noetherian); in a PID R any nonzero prime ideal is maximal and the gcd of $a_1, \ldots, a_n$ is an R-linear combination of $a_1, \ldots, a_n$.

KNOW ZORN'S LEMMA If S is a nonempty partially ordered set such that every chain (linearly ordered subset) C has an upper bound ($b \in S$ with $b \geq c$ for all $c \in C$), then S has at least one maximal element m ($t \in S$, $t \geq m \Rightarrow t = m$).
Main application in ring theory: Any proper ideal I of a ring R is contained in a maximal ideal M of R. (The important special case $I = \{0\}$ yields the existence of maximal ideals.)

AVOID THE FOLLOWING MISTAKES: If $\phi : R \longrightarrow S$ is a ring homomorphism and I is an ideal in R, $\phi(I)$ needn't be an ideal in S (it is if ϕ is surjective), and if I is prime (or maximal) in R, the ideal generated by $\phi(I)$ in S need **not** be prime (or maximal) in S (even if ϕ is surjective); $\mathbb{Z}[x]$ does **not** admit a Euclidean algorithm (it's even not a PID), similarly with $K[x, y]$ where K is a field; if in a domain R the gcd of two elements a and b exists and equals 1, this does **not** imply that the ideal (a, b) equals R (it does if (a, b) is principal).

RELATED PROBLEMS

(Unless otherwise stated, all rings R are commutative with unit 1; F denotes a field.)

1. (April 77 #4) (a) If M is a maximal ideal, SHOW R/M is a field. (Done.)
   (b) If R is a Euclidean domain, show every ideal generated by an irreducible element is maximal.

2. (May 78 #5) Is the ring $C[0, 1]$ of continuous real-valued functions on the closed interval [0,1] noetherian?

3. (Sep 78 #6) R is called a *local ring* if it has a unique maximal ideal; a domain is called a *valuation domain* if for every two elements a, b either a divides b or b divides a. (a) Show R is local iff the non-units form an ideal M. (b) Show every valuation domain is local. (c) Show a local ring has no idempotents ($e^2 = e$) other than 1,0.

4. (Sep 79 #7a; Nov 77 #5) Give two examples of non-noetherian rings.

5. (May 80 #2) Hilbert's Theorem says that $F[x_1, \ldots, x_n]$ is noetherian. Show that ANY finitely generated commutative F-algebra A is noetherian.

6. (Jan 82 #6) If I is an ideal of R with $I \cap S = \emptyset$ for some multiplicatively closed subset S of R containing 1, show there exists an ideal M of R containing I and maximal with respect to $M \cap S = \emptyset$. Find an M if $R = \mathbb{Z}$, $S = \{3^n \mid n \geq 0\}$, $I = 2\mathbb{Z}$.

7. (Mar 83 #8) Does 7 divide $10^{31} + 31^{10}$? Why?

8. (Feb 84 #3) If R is finite, show every prime ideal is maximal.

9. (1985 #3c) If a, b are relatively prime integers, show the ring $\mathbb{Z}_{ab}$ is isomorphic to the direct sum $\mathbb{Z}_a \oplus \mathbb{Z}_b$ of rings. Show (in ≤ 1 word) why this implies if $m = p_1^{e_1} \ldots p_t^{e_t}$ that $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{e_t}}$.

10. (May 89 #7; Aug 97 #8c) Show an element $a \in R$ belongs to $J = \bigcap\{\text{maximal ideals of } R\} \iff 1 + ra$ is a unit for all $r \in R$.

11. (May 1990 #5) If R is an integral domain with only finite number n of ideals, show R is a field, and give an upper bound for n.

12. (May 92 #2) If a, b in an integral domain R satisfy $a^n = b^n,\ a^m = b^m$ for m and n relatively prime, show $a = b$. (Do you need that R is an integral domain?)

13. (Jan 92 #6) Prove that an integral domain has the descending chain condition on ideals iff it is a field.

14. (Sept 93 #2) If P is a prime ideal which is *not* maximal, show P has infinitely many cosets in R.

15. (Sept 93 #5) (a) Let D be a Euclidean domain, with Euclidean function δ (but do not assume $\delta(ab) \geq \delta(a)$). Let $D_n = \{a \in D \mid a \neq 0 \text{ and } \delta(a) \geq n\}$. Show that (i) if $b \in D_0$ and there exists an $a \in D$ such that $a + Db \subseteq D_n$, then $b \in D_{n+1}$; (ii) $\bigcap_n D_n = \emptyset$.
(b) Conversely, show that if an integral domain D has a chain of subsets $D\backslash\{0\} = D_0 \supseteq D_1 \supseteq D_2 \supseteq \ldots$ satisfying properties (i) and (ii), then D is Euclidean.

16. Let R be an integral domain, $N : R\backslash\{0\} \longrightarrow \{n > 0 \mid n \in \mathbb{Z}\}$ be a function for which (i) $N(1) = 1$ and (ii) $N(xy) = N(x)N(y)$ for all x, y in $R\backslash\{0\}$.
(a) Let K be the field of fractions of R. Show that N can be extended in a unique way to a function from $K\backslash\{0\}$ into $\mathbb{Q}$ that still satisfies (i) and (ii) (now for all $x, y \in K \setminus \{0\}$).
(b) Show that R is a Euclidean domain under N iff for each $x \in K\backslash\{0\}$ there is an element $r \in R$ for which $N(x - r) < 1$.

17. (Jan 94 #8) Let ZD denote the set of zero divisors of R (including 0). Let $\mathcal{I}$ be the set of ideals of R which are contained in ZD.
(a) Show that $R \setminus ZD$ is closed under multiplication
(b) Show that if M is a maximal member of $\mathcal{I}$, then M is a prime ideal.
(c) Use Zorn's Lemma to show that each member of ZD is contained in a maximal member of $\mathcal{I}$.
(d) Conclude that the set ZD is a union of prime ideals.

18. (Aug 97 #8) (a) Show that the set N of all nilpotent elements z ($z^n = 0$ for some n) of R forms an ideal (called the *nil radical* of R).
(b) The intersection J of all maximal ideals of R is called the *Jacobson radical* of R; show that $N \subseteq J$.
(c) Give an example where N and J are different.

19. (Aug 99 #4) If R is an integral domain, find all R-linear automorphisms of the polynomial ring $R[x]$. (If you can't do the general case, do the case when $R = F$ is a field.)

20. (Aug 02 #5) Let R be a commutative ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of R. If for all $i \neq j$ we have $\mathfrak{a}_i + \mathfrak{a}_j = R$ then $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$. (*Hint.* Induct, starting from $n = 2$.)

21. (Aug 02 #8) Is it true that in the ring R of all continuous real-valued functions on $[0,1]$, any element which is not a zero divisor, is invertible?
And (May 03 #6): Give an example of a maximal ideal in R.
And (Jan 06 #4): Is this maximal ideal principal?

22. (Aug 05 #3) Let R be a commutative ring with 1 (not necessarily a domain) such that any ideal in R is principal. Let $S \subseteq R$ be a multiplicatively closed subset of R. Show that any ideal in the ring of fractions $S^{-1}R$ is also principal.

23. (Aug 06 #5) Let R be a commutative ring. A *radical* is an ideal $I \trianglelefteq R$ such that, for any $a \in R$, we have $a \in I$ whenever some power $a^k \in I$.
(a) Show that every prime ideal is radical.
(b) Assume I is radical and $a \in R$ does *not* lie in I. Show that there exists a prime ideal P that contains I but does not contain a. (Hint: use Zorn's lemma.)

24. (Aug 08 #5) Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers, and let $I = (a, b)$ be the ideal generated by $a = 16i, b = 5 + 3i$ in R.
a. Systematically find $c \in R$ such that $I = (c)$.
b. Prove or disprove: R/I is a finite field.

25. (Jan 09 #4) (a) Prove that the ring of Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain.
(b) Let n and m be positive integers and assume that m is a product of distinct primes. Prove that the polynomial $f(x) = x^n - m$ is irreducible in $\mathbb{Q}[x]$.

26. (Jan 12 # 3) Let $R = \mathbb{Z}[\sqrt{-2}]$.
(a) Prove that R is a Euclidean domain. Hint: Use the square of the usual complex norm.
(b) Write 7 and 11 as products of irreducible elements of R. Justify your answer.

27. (Aug 12 # 4) Let R be a commutative ring with 1. Let N be the nilradical of R, that is, N is the set of all nilpotent elements of R (including 0). You may use without proof that N is the intersection of all prime ideals of R. Prove that the following conditions are equivalent:

    (i) R has just one prime ideal.

    (ii) R/N is a field.

28. (Jan 13 #2) In both parts of this problem R is a commutative domain with 1 and K is the field of fractions of R.

    (a) Let $R = \mathbb{Z}[t]$, the ring of polynomials over $\mathbb{Z}$ in one variable. Let $p(x) = x^n + r_{n-1}x^{n-1} + \ldots + r_0 \in R[x]$ be a monic polynomial with coefficients in R, and suppose that $p(\alpha) = 0$ for some $\alpha \in K$. Prove that $\alpha \in R$.

    (b) Now let $R = \mathbb{Z}[\sqrt{-3}]$. Find a monic polynomial $p(x) \in R[x]$ which has a root in K, but has no root in R (and prove that $p(x)$ has required properties). **Hint:** There actually exists a quadratic polynomial with integer coefficients with required property.

29. (Jan 14 #2) Find all ring homomorphisms

    (a) from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$;

    (b) from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}$.

30. (Jan 14 #3) Let $\mathbb{Q}(\sqrt{-2})$ be a quadratic field with associated ring of integers $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$. Prove that $\mathcal{O}$ is a Euclidean Domain . (Hint: use the field norm.)

31. (Jan 14 #4) Prove that if R is a principle ideal domain (P.I.D.) and D is a multiplicatively closed subset of R with $0 \notin D$, then $D^{-1}R$ is also a P.I.D.

32. (Aug 15 #1) Find all maximal ideals of $\mathbb{Z}[i]$ which contain 182. Find minimal generators for these ideals.

33. (Aug 16 #6) (a) Name two examples of each of the following: (i) PIDs which are not fields (ii) UFDs which are not PIDs (iii) commutative integral domains which are not UFDs and (iv) commutative rings which are not integral domains, (v) noncommutative rings.
    (b) Given an example of a non-principal ideal in one of the examples you listed (with proof).

34. (Aug 17 #4) Let R be a commutative ring with 1 which is *Artinian*, i.e. for any descending chain $I_1 \supseteq I_2 \ldots \supseteq I_n \ldots$ of ideals of R there exists an n_0 such that $I_n = I_{n_0}$ for all $n \geq n_0$. Prove the following:
    (a) If R is an integral domain, then it is a field.
    (b) Any prime ideal of R is maximal.
    (c) R has only finitely many maximal ideals.

    Here are some further standard facts/problems concerning rings of fractions (S always denotes a multiplicatively closed subset of R containing 1).

35. Show that the prime ideals of $S^{-1}R$ are in one-to-one correspondence with the prime ideals of R not containing any element of S. Is a similar statement true for maximal ideals?

36. Show that $S^{-1}R$ is a local ring (i.e. has precisely one maximal ideal) if $S = R \setminus P$ for a prime ideal P of R. In this case we use the notation $R_P := S^{-1}R$.

37. Prove that R does not have any nonzero nilpotent elements if and only if, for all prime ideals P, R_P does not have any nilpotent elements.

38. Suppose that $S = \{a^n \mid n \in \mathbb{N}_0\}$ ($a^0 := 1$) for some $a \in R \setminus \{0\}$. Show that $S^{-1}R$ is isomorphic to $R[x]/(ax - 1)$. What does this mean for nilpotent a?

2.2 PID's, UFD's and polynomial rings

KNOW: how to compute the gcd and the lcm of two elements a and b in a UFD R and that the gcd can in general **not** be written as an R-linear combination of a and b (as opposed to the case

where R is a PID); standard examples of non-principal ideals in $\mathbb{Z}[x]$ and $K[x,y]$ for a field K; the difference between irreducible and prime elements (for instance in a ring like $\mathbb{Z}[\sqrt{-5}]$) and that these two notions coincide in a UFD; the fact that prime elements generate prime ideals which are minimal among the nonzero prime ideals if R is a UFD; the fact that in any integral domain irreducible elements generate principal ideals which are maximal among the proper principal ideals.

KNOW HILBERT'S BASIS THEOREM: If R is Noetherian, then also the polynomial ring $R[x]$ is Noetherian, i.e. all its ideals are finitely generated.

KNOW GAUSS' LEMMA AND ITS VARIANTS: If R is a UFD, $f, g \in R[x]$ with f primitive and $f \mid g$ in $F[x]$, where F is the field of fractions of R, then $f \mid g$ in $R[x]$; primitive polynomials of $R[x]$ are irreducible iff they are prime in $R[x]$ iff they are irreducible (or prime) in $F[x]$;
Consequence: $R[x]$ is also a UFD, in particular $\mathbb{Z}[x_1, \ldots, x_n]$ and $K[x_1, \ldots, x_n]$ are UFD's for any $n \in \mathbb{N}$ and any field K.

KNOW EISENSTEIN'S CRITERION: If $f \in R[x]$ is a primitive polynomial (R a UFD) and p a prime dividing all coefficients of f but the leading one and p^2 not dividing the constant term, then f is irreducible in $R[x]$ and hence in $F[x]$.

AVOID THE FOLLOWING MISTAKES: If R is a subring of S and p is a prime element in R, p need **not** be a prime element in S (even if S is a UFD and p is not a unit in S); if you want to deduce from an equation $a = bc$ in a domain R that a is not irreducible, don't forget to check that a and b are no units in R; likewise, if you have different irreducible elements a, b, c, d in R and you want to deduce from an equation $ab = cd$ that they are not prime in R, don't forget to check that they are not associate; keep in mind that the primitivity of f is an important assumption in Gauss' Lemma; don't apply Eisenstein's criterion to $\mathbb{F}_q[x]$ ($\mathbb{F}_q$ is not the field of fractions of a proper subdomain, and it doesn't have any prime elements).

RELATED PROBLEMS

(Unless otherwise stated, all rings R are commutative with unit 1; F denotes a field.)

1. (April 77 #4) (a) If M is a maximal ideal, SHOW R/M is a field.
   (b) If R is a Euclidean domain, show every ideal generated by an irreducible element is maximal.

2. (Jan 79 #2; May 91 #2a) (a) SHOW that any Euclidean domain is a PID.
   (b) Show that any two nonzero elements have a g.c.d. in R if R is a Euclidean domain.
   (c)Find (systematically) $m, n \in \mathbb{Z}$ so that $421m + 1664n = 1$.

3. (Sep 79 #7b) Given an example of a prime ideal in R which is *not* maximal; is there an example where R is a UFD?

4. (Sep 80 #2) (a) Give 3 examples of PIDs.
   (b) Show that the homomorphic image of a PIR (Principal Ideal Ring: all ideals are principal, but perhaps not a domain) is again a PIR.
   (c) Give an example of a PID with a homomorphic image which is not a PID.

5. (Jan 81 #4) SHOW $F[x]$ is a Euclidean domain, but $F[x, y]$ is *not*.

6. (Sep 82 #2) If $a_1, \ldots, a_n$ in a PID R have gcd d, show that there exists an invertible $n \times n$ matrix Q of determinant 1 over R with $Q\,[a_1, \ldots, a_n]^T = [d, 0, 0 \ldots 0]^T$. (This is false if R is merely a UFD).

7. (Mar 83 #5) If D is a UFD whose units together with 0 form a proper subring U, show D has infinitely many (nonassociate) primes. Give an example of such a D.

8. (Sep 83 #7) If $R \subseteq S$ are PIDs with $d = \gcd_R(a, b)$, show $d = \gcd_S(a, b)$ too.

9. (Feb 84 #5) Factor $x^3 - y^3$ into irreducible factors in $\mathbb{Q}[x, y]$.

10. (1985 #3a) Show $x^5 - 6x^3 + 12x^2 + 21x - 3$ is irreducible in $\mathbb{Q}[x]$.

11. (Jan 87 #5) If R is an integral domain, what are necessary and sufficient conditions that $R[x]$ be: (0) a domain, (1) a PID, (2) a UFD, (3) noetherian.

12. (Fall 87 #2) Prove or disprove: R PID $\Longrightarrow R[x]$ is PID.

13. (Aug 88 #1) If F is a field, PROVE $F[x]$ is a PID.

14. (Jan 89 #6) Prove or disprove: Every UFD is a PID.

15. (Aug 89 #4) Show $R = \{f(x) \in \mathbb{Z}[x] \mid$ the coefficient of x in $f(x)$ is even$\}$ is a subring. Show that 2 and $2x$ have a g.c.d. in R, but not a l.c.m.

16. (May 1990 #4) If P is a nonzero prime ideal in a UFD, show P is minimal among nonzero prime ideals iff P is a principal ideal.

17. (May 91 #2b) Prove or disprove: R Euclidean domain $\Longrightarrow R[x]$ Euclidean domain and/or any two nonzero elements of $R[x]$ have a g.c.d. in $R[x]$.

18. (Jan 92 #2) Show that a polynomial of degree n over F has at most n roots in F.

19. (May 92 #6) Show that $f(x, y) = x + x^3y + y^8 + x^7y^5 + x^2y^4$ is irreducible over the rational field.

20. (Jan 94 #3) Prove that $y^3 + x^2y^2 + x^3y + x$ is irreducible in $\mathbb{Z}[x, y]$.

21. (Aug 94 #3) Describe which polynomials in $\mathbb{R}[x]$ belong to the subring $\mathbb{R}[x^2, x^3]$, $\mathbb{R}$ the field of real numbers.

22. (Jan 95 #6) Prove that any proper homomorphic image of a PID that remains an integral domain must actually be a field.

23. (Aug 95 #4) Show that $\mathbb{Z}[\sqrt{10}] = \mathbb{Z} + \mathbb{Z}\sqrt{10}$ is not a UFD. (Hint: show that a) $n^2 - 10m^2 \neq \pm 2, 3$ for all $n, m \in \mathbb{Z}$, b) 2, 3, and $4 \pm \sqrt{10}$ are irreducible in $\mathbb{Z}[\sqrt{10}]$.)

24. (Aug 95 #5) Factor $x^9 - x$ in $\mathbb{F}_3[x]$ into irreducible factors ($\mathbb{F}_3$ the Galois field of three elements).

25. (Aug 96 #4) In $\mathbb{Q}[x]$, let $f(x) = x^{m_1} + \ldots + x^{m_k}$ where $m_i \equiv i - 1 \pmod{k}$. Show that $f(x)$ is divisible by $x^{k-1} + x^{k-2} + \ldots + 1$.

26. (Aug 96 #5) Let R be a PID. An ideal P of R is called *primary* if whenever $ab \in P$ and $a \notin P$ then $b^n \in P$ for some n (depending on b). Show that P is primary iff either $P = 0$ or $P = (p^m)$ for some prime $p \in R$ and some exponent m.

27. (Jan 97 #4) Give counterexamples for each of the following statements, with details. Then correct each statement by modifying the underlined part. (a) If R is a commutative ring, then a polynomial in $R[x]$ of degree n has at most n roots in R. (b) If R is a division ring, then a polynomial in $R[x]$ of degree n has at most n roots in R. (c) If R is a unique factorization domain, then the greatest common divisor d of two members a, b of R can be written as $d = ax + by$ for some x and y in R.

28. (Jan 98 #3) Let R be a PID. If a, b are two nonzero elements in R, show that they have a l.c.m. (an element $m \in R$ such that (1) $a, b \mid m$, (2) if $a, b \mid x$ then $m \mid x$.)

29. (August 98 #5) The *Krull dimension* of a commutative ring R is the longest chain of prime ideals properly contained in R, i.e. the largest integer n such that there exists a chain $P_0 < P_1 < \ldots < P_n < R$ ($P_0 = 0$ allowed if prime) of *prime ideals* P_i in R. If R is a PID, find its Krull dimension.

30. (Jan 00 #6) Given a finite field K, *show* there exists a polynomial $f(x, y) \in K[x, y]$ (in which both variables actually appear) for which the equation $f(x, y) = 0$ has no solutions in $K \times K$.

31. (Aug 01 #4) If x is an element of a PID R, show that the left R-module R/Rx is irreducible as a *module* if and only if the element x is irreducible as an *element*.

32. (Aug 02 #1) (a) Find all nonconstant polynomials $p(x) \in \mathbb{C}[x]$ satisfying $p(p(p((x)) = p(x)$. (b) Find all rational functions $\varphi(x) \in \mathbb{C}(x)$ satisfying $\varphi(2x) = \varphi(x)$.

33. (Aug 02 #6) Let $R = \mathbb{C}[x, y]/\mathfrak{a}$ where $\mathbb{C}[x, y]$ is the ring of polynomials in variables x and y, and $\mathfrak{a}$ is the principal ideal of $\mathbb{C}[x, y]$ generated by $p(x, y) = y^2 - x^3$. Show that the ideal of R generated by the image of x and y is not principal.

34. (May 03 #7) Let $f(x) \in \mathbb{R}[x]$ be a nonzero polynomial. Show that there exists a number $r \in \mathbb{R}$ such that the polynomials $f(x)$ and $f(x + r)$ are relatively prime.

35. (Aug 03, #2) Let D be a PID with F as its field of fractions. Show that every element $x \in F$ can be written as a sum of *primary fractions* (i.e. with denominators powers of primes):

$$x = \sum_{i=1}^{n} \frac{a_i}{p_i^{e_i}}$$

for some $a_1, \ldots, a_n \in D$ and non-associate primes $p_1, \ldots, p_n \in D$.

36. (Jan 04 #4) Show that a principal ideal in $\mathbb{Z}[x]$ can never be maximal.

37. (Aug 04 #3) Consider the ring $R = \mathbb{Z}[\sqrt{-7}] = \{m + n\sqrt{-7} \mid m, n \in \mathbb{Z}\}$.
(a) Is R a UFD? Give arguments for your answer.
(b) Exhibit an ideal I in R which is not principal. *Show* that your I is not principal.

38. (Jan 05 #5) Prove that the ideal $(x^2 + 2, x^2 + 7)$ is maximal in $\mathbb{Z}[x]$.

39. (Jan 06 #8) For an element $a \in \mathbb{Q}$, consider the homomorphism φ from the polynomial ring $\mathbb{Q}[x]$ to the ring $M_3(\mathbb{Q})$ of 3×3 matrices, given by evaluation $f(x) \mapsto f(A)$ for

$$A = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}.$$

Show that the kernel of φ is the set of all polynomials $f(x)$ with $f(a) = f'(a) = f''(a) = 0$. Is this a principal ideal?

40. (Aug 06 #4) Decide whether

$$xy^2 + x^2y + 2xy + y + x + 1$$

is irreducible in $\mathbb{Q}[x, y]$.

41. (Aug 06 #7) Determine the number of monic irreducible polynomials of degree 2 in $\mathbb{F}_7[x]$.

42. (Jan 08 #4) (a) If $r \in \mathbb{Q}$ is a rational root of a monic integral polynomial

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

show that $r \in \mathbb{Z}$ is integral.
(b) Factor $y^5x + y^3x^2 + y + x^3$ into irreducible factors in $\mathbb{Z}[x, y]$, explaining why each is irreducible.

43. (Jan 08 #5) Let R be a unital commutative ring, and consider 5 possible properties such a ring might have: it is $(\mathcal{P}_1)$ a domain, $(\mathcal{P}_2)$ a PID, $(\mathcal{P}_3)$ Euclidean, $(\mathcal{P}_4)$ noetherian, $(\mathcal{P}_5)$ a UFD.
(a) For which n is it true that $R[x]$ *always* inherits property $(\mathcal{P}_n)$ from R (if R has $(\mathcal{P}_n)$, so *must* $R[x]$)? Circle the $n's$ for which this holds, and explain your answer or give a counterexample.

$n =$	1	2	3	4	5

(b) For which n is it true that R inherits property $(\mathcal{P}_n)$ from $R[x]$? Circle the $n's$ for which this holds, and explain your answer or give a counterexample.

$n =$ | 1 | 2 | 3 | 4 | 5 |

(c) For which $n \neq 5$ is it true that a quotient R/P of R by a prime ideal ($P \lhd R, P \neq R$) inherits property ($\mathcal{P}_n$) from R? Circle the $n's$ for which this holds, and explain your answer or give a counterexample.

$n =$ | 1 | 2 | 3 | 4 |

44. (Jan 08 #6) Let $R = \mathbb{Z} + 2\mathbb{Z}[x] = \mathbb{Z}1 + \sum_{n=0}^{\infty} 2\mathbb{Z}x^n$.
(a) Show that R is not a UFD by finding an irreducible element that is not prime.
(b) Show that R is not noetherian by showing that the ideal $2\mathbb{Z}[x]$ is not finitely generated: $2\mathbb{Z}[x] \neq \sum_{i=1}^{n} Rf_i(x)$ for any $f_i(x) \in 2\mathbb{Z}[x]$.

45. (Jan 09 #3) Let F be a field, and let R be the subring of $F[x]$ consisting of all polynomials with zero coefficient of x, that is,

$$R = \{a_0 + a_2x^2 + \ldots + a_nx^n : a_i \in F\}.$$

(a) Prove that the elements x^2 and x^3 are irreducible but not prime in R.
(b) Is R a principal ideal domain? Prove your answer.
(c) Prove that R is Noetherian.

46. (Aug 09 #3)(a) Let R be a principal ideal domain and $I \subset R$ a proper nonzero ideal. Prove that if the quotient ring R/I is a domain then it must be a field.
(b) Does the assertion of (a) remain true if R is only assumed to be a unique factorization domain? Prove or give a counterexample.

47. (Aug 09 #4) Let F be a field and $R = F[x, y]$ the ring of polynomials in two (commuting) variables x and y. Let $I = xR$ be the principal ideal of R generated by x and $S = F + I = \{f + i : f \in F, i \in I\}$. Observe that S is a subring of R and I is an ideal of S (you need to justify these facts).
(a) Prove that I is not finitely generated as an ideal of S.
Hint: Assume that I is finitely generated as an ideal of S and reach a contradiction by showing that there must exist a natural number m such that any polynomial $p(x, y) \in I$ contains no monomials of the form xy^n, with $n > m$.
(b) Prove that S is not finitely generated as a ring.
Hint: It is possible to answer (b) using (a) without doing any computations.

48. (Aug 10 #3) Let $\mathbb{R}$ denote the real numbers. The purpose of this problem is to show that the ring $A = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$ is not a UFD. For an element $f \in \mathbb{R}[x, y]$ we denote its image in A by $[f]$.
(a) Show that every element of A can be uniquely expressed in the form $[f(x) + g(x)y]$ where $f(x), g(x) \in \mathbb{R}[x]$.

(b) Show that A has an automorphism φ of order 2 such that $\varphi([f(x)]) = [f(x)]$ for each $f(x) \in \mathbb{R}[x]$ and $\varphi([y]) = -[y]$.
(c) Use (a) and (b) to construct a function $N : A \to \mathbb{R}[x]$ such that $N(uv) = N(u)N(v)$ for all $u, v \in A$.
(d) Use the function N from (c) to show that $[x]$ is an irreducible element of A and that the only invertible elements of A are (images of) nonzero constant polynomials.
Hint: It is essential that you are working over $\mathbb{R}$, not over $\mathbb{C}$.
(e) Now show that A is not a UFD.

49. (Aug 10 #4) Recall that a ring S is called *graded* if $S = \oplus_{n=0}^{\infty} S_n$ where each S_n is an additive subgroup and $S_n \cdot S_m \subseteq S_{n+m}$ for all n, m. An element $s \in S$ is called *homogeneous* if $s \in S_n$ for some n. An ideal I of S is called a *graded ideal* if $I = \oplus_{n=0}^{\infty}(I \cap S_n)$.
(a) Let S be a graded ring and I and ideal of S. Prove that I is a graded ideal if and only if I is generated (as an ideal) by a set of homogeneous elements.
(b) Let R be a commutative ring with 1 and $S = R[x]$. Then S is a naturally graded ring where $S_n = \{rx^n : r \in R\}$. Assume that there exists $k \in \mathbb{N}$ such that every ideal of R can be generated by at most k elements.
Let I be a graded ideal of S. Prove that I can be written as $I = J \oplus M$ where J is an ideal of S generated by at most k elements and M is a finitely generated R-module.
Hint: Adapt the proof of Hilbert's basis theorem.

50. (Aug 11 # 4a) Find all the irreducible polynomials of degree 4 over the finite field $\mathbb{F}_2$.

51. (Jan 12 # 7) If q is a prime power, denote by $\mathbb{F}_q$ a finite field of order q.
(a) Find a monic irreducible polynomial of degree 3 over $\mathbb{F}_5$ and use it to construct a field of order 125. Justify your answer.
(b) Find all q for which the polynomial $p(x) = x^2 + x + 1$ is irreducible in $\mathbb{F}_q[x]$. Hint: What can you say about roots of $p(x)$, and what do you know about the multiplicative group $\mathbb{F}_q^{\times}$?

52. (Aug 12 #3) Let k be a field and $R = k[x, y]/(x^5 - y^2)$.

    (a) Prove that R is isomorphic to the subring $k[t^2, t^5]$ of $k[t]$ (the polynomials in one variable over k).

    (b) Prove that R is not isomorphic to $k[t]$ (as a ring).

53. (Jan 13 #3) Let F be a field, d a positive integer, and $f_1, f_2, \ldots \in F[x_1, \ldots, x_d]$ an infinite sequence of polynomials in $F[x_1, \ldots, x_d]$. Given a positive integer n, let S_n be the set of all d-tuples $(a_1, \ldots, a_d) \in F^d$ satisfying the following system of equations:

$$f_i(a_1, \ldots, a_d) = 0 \text{ for each } 1 \leq i \leq n-1 \text{ and } f_n(a_1, \ldots, a_d) = 1.$$

    Prove that there exists an integer N such that the set S_n is empty for all $n \geq N$. **Hint:** Noetherian rings.

54. (Aug 15 #2) Let r_1, r_2, r_3 be the roots of the cubic polynomial $X^3 + 10X^2 - 5X + 4$. Find the cubic polynomial with rational coefficients whose roots are r_1^2, r_2^2, r_3^2.

55. (Jan 16 #1) Let K be a field (possibly finite). Prove that the polynomial ring $K[X]$ has infinitely many maximal ideals.

56. (Aug 17 #5) Let $R = \mathbb{Z}[x]/(x^3 + x^2 + 1)$ be the quotient of the polynomial ring $\mathbb{Z}[x]$ modulo the principal ideal $(x^3 + x^2 + 1)$.
(a) (4 points) Is R an integral domain?
(b) (8 points) Which of the principal ideals $(2), (3), (5)$ of R are prime ideals? And which of them are maximal?

57. (Jan 18 #2) Consider the ring $R = \mathbb{Z}[\sqrt{-11}] = \{m + n\sqrt{-11} \mid m, n \in \mathbb{Z}\}$.
(a) Is R a UFD? Give arguments for your answer.
(b) Exhibit an ideal I in R which is not principal. *Show* that your I is not principal.

58. (Jan 18 #3) Decide in each of the following three cases whether the given polynomial is irreducible. Include arguments.
(a) $x^2 - 2i$ in $\mathbb{Z}[i][x]$;
(b) $x^3 - 49x^2 + (3 + \sqrt{2})x + 7$ in $\mathbb{Z}[\sqrt{2}][x]$;
(c) $x^2 + xy + y^2$ in $\mathbb{C}[x, y]$.

2.3 Non-commutative rings

In Algebra I and II, no serious non-commutative ring theory is covered, which is the main subject of Algebra III. A few very basic notions you should know anyhow.

KNOW BASIC RING DEFINITIONS: Ring, subring; (group of) units, divison ring (or skew field); zero divisors; left-, right- and two-sided ideals; quotient *module* R/I for a left ideal I and quotient *ring* R/I for a two-sided ideal I; (side remark: the existence of maximal left-, right- and two-sided ideals again follows from Zorn's Lemma); ring homomorphisms and isomorphisms; center $Z(R)$ of a ring R; K-algebra for a field K.

KNOW TWO BASIC EXAMPLES: the Hamiltonian quaternions $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$; the matrix algebra $M_n(K)$ for a field K.

RELATED PROBLEMS

(R here is a not necessarily commutative ring with unit 1)

1. (Nov 77 #10) Let F be a field of characteristic $p > 0$. A *p-polynomial* is a polynomial $f(x) = a_n x^{p^n} + \ldots + a_1 x^{p^1} + a_0 x^{p^0} = a_n x^{p^n} + \ldots + a_1 x^p + a_0 x$ which is a linear combination of p^e-th powers of x ($e = n, .., 1, 0$). If $a_n \neq 0$ then f has *degree n.*
(a) Show that the set R of all p-polynomials becomes a non-commutative ring under the usual addition and the substitution product $f(x) * g(x) = f(g(x))$. Does R have a unit element? What are the zero divisors?
(b) Show that every left ideal I in R is principal, $I = Rf$.
(c) Show that every right ideal of R is principal iff the field F is perfect ($F^p = F$).
(d) Are there any perfect fields F for which R is commutative?

2. (Sep 84 #2) Let L be a left ideal in R.
(a) Show $I(L) = \{a \in R \mid La \subseteq L\}$ is the largest subring S of R such that L is a 2-sided ideal of S.
(b) Prove that R is a division ring iff $I(L) = L$ for all nonzero L.

3. (1985 #3d) An element of R is nilpotent if $x^n = 0$ for some n. Show that if x, y are commuting nilpotent elements in R then so is $x + y$; give an example to show this is not true if x, y do not commute.

4. (Sep 86 #7) (a) Define the quaternions $\mathbb{H}$ over the reals.
(b) Show that any homomorphism of $\mathbb{H}$ into the complex numbers is identically zero.
(c) Prove that the equation $x^2 + 1 = 0$ has infinitely many solutions in $\mathbb{H}$. Why can't you deduce from the "factorization" $x^2 + 1 = (x + i)(x - i)$ and the fact that $\mathbb{H}$ is a division ring that there are only two solutions?
(d) How many solutions has the equation $x^2 - 1 = 0$ in $\mathbb{H}$?

5. (May 89 #2) Show that in a general ring (not necessarily commutative or with unit), all the elements that are not divisors of zero have the same additive order. What are the possible values for this order?

6. (Aug 89 #2) If $(a + b)^2 = a^2 + b^2$ for all a, b in R, show R is commutative.

7. (Jan 94 #5) Give an example (and a proof that it works) of a ring R without identity and an ideal in the ring direct sum $R \oplus R$ that does *not* have the form $I_1 \oplus I_2$ where the I_k are ideals in R.

8. (Aug 98 #5) A *derivation* D of a ring R is a map of R into itself such that $D(a + b) = D(a) + D(b)$ and $D(ab) = D(a)b + aD(b)$ for all elements a, b of R. Show that if D is a derivation, and in addition $D^2 = 0$ and R has no 2-torsion ($2a = 0$ implies $a = 0$), then the "exponential map" $Id + D$ is an *automorphism* of R.

9. (Jan 05 #4) Let K be a field and A a finite-dimensional K-algebra (that is A is a ring with 1 containing K in its center with $\dim_K A < \infty$). Show that any element of A is either a zero divisor or a unit.

10. (Aug 10 #7) Let K be a field. Let A be a finite-dimensional (possibly non-commutative) K-algebra (with 1), and assume that A is a division ring.
(a) Prove that every K-subalgebra of A is a division ring.
(b) Assume that K is algebraically closed. Prove that $\dim_K A = 1$.

11. (Aug 11 # 1) Let M be a simple (left) module for a ring R. This means that M has no submodules apart from 0 and M.
(a) Prove that $M \cong R/I$ where I is a maximal left ideal of R.
(b) Show that $E := \mathrm{End}_R(M)$ is a division ring, i.e., every nonzero element of E is invertible.

12. (Jan 12 # 4) Let R be a ring with 1. The opposite ring R^{op} is defined as follows: as a set $R^{op} = R$, the addition on R^{op} coincides with the addition on R and the multiplication $*$ on R^{op} is the multiplication on R in reverse order, that is, $a * b = ba$ (where ba is the product in R). Let $e \in R$ be an idempotent element, that is, $e^2 = e$.

(a) Prove that $eRe = \{ere : r \in R\}$ is a ring with multiplicative identity e.
(b) Consider the left R-module M = Re. Prove that its endomorphism ring $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is isomorphic to $(eRe)^{op}$, the opposite ring of eRe.

13. (Aug 14 #8) Let $A = M_n(R)$ be the algebra of $n \times n$ matrices over a commutative ring R with 1. Fix $1 \leq i, j \leq n$. Determine
(a) the left ideal of A generated by E_{ij};
(b) the (two-sided) ideal of A generated by E_{ij};
(c) Are there possibly other nonzero ideals of A besides those of the form (b)?
(Here as usual E_{ij} denotes the matrix whose (i, j)th entry is 1 and 0 elsewhere.)

14. (Jan 17 #8) Let A be the ring of $n \times n$ matrices over a field F.

(a) Show the right ideals of A are precisely the subsets of the form

$$\{X \in A \mid \mathrm{image}(X) \subset V\}$$

where V ranges over all linear subspaces of F^n.

(b) Show the left ideals of A are precisely the subsets of the form

$$\{X \in A \mid \mathrm{kernel}(X) \supset W\}$$

where W ranges over all linear subspaces of F^n.

(c) Show that A is a simple ring: its only 2-sided ideals are A itself, and $\{0\}$.

Chapter 3

Modules and canonical forms

3.1 Modules

KNOW BASIC NOTIONS:
(i) for a general, not necessarily commutative ring R:
R-module, submodule, quotient module, isomorphism theorem(s), correspondence theorem; annihilators and torsion elements; cyclic, simple (or irreducible) and free modules; direct sums and direct products and their universal properties; know that the direct product of infinitely many copies of $\mathbb{Z}$ is **not** a free $\mathbb{Z}$-module; spanning and linearly independent subsets; sets of R-module homomorphisms and the algebraic structures on them: $\mathrm{Hom}_R(M, N)$ is always an abelian group and an R-module if R is commutative; $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is always a ring and an R-algebra if R is commutative; know that $\mathrm{End}_R(R^n)$ is isomorphic to $M_n(R)$;
(ii) for an integral domain R: torsion submodule; well-defined rank of a free R-module; know that submodules of free modules need **not** be free but that rk $M' \leq$ rk M if M' is a free submodule of a free module M.

KNOW THE BASIC THEOREMS FOR FINITELY GENERATED MODULES OVER A PID R: submodules of a free R-module M are free (this is also true if M is not finitely generated); torsion free finitely generated R-modules are free; a finitely generated R-module M is always the direct some of its torsion submodule $T(M)$ and a free (finitely generated) submodule, and $T(M)$ is a finite direct sum of cyclic modules; existence and uniqueness of invariant factors and elementary divisors, namely (see also Section 1.3):

Elementary Divisor Form (longest decomposition into cyclics): Any finitely generated R-module M can be written as $M = R/(p_1^{e_1}) \oplus \ldots R/(p_r^{e_r}) \oplus R^n$, where n is the rank of $M/T(M)$, the p_i are (not necessarily distinct) prime elements of R, determined up to multiplication with units by M, and the e_i are natural numbers, also uniquely determined by M (up to possible permutations of the direct summands). The prime powers $p_i^{e_i}$ $(1 \leq i \leq r)$ are called the *elementary divisors* of M.

Invariant Factor Form (shortest decomposition into cyclics): $M = R/(d_1) \oplus \dots R/(d_s) \oplus R^n$ with n as before and elements $d_i \in R \setminus (R^* \cup \{0\})$ satisfying $d_1 \mid d_2 \dots \mid d_s$. These elements d_i are, up to multiplication with units, uniquely determined by M and called the *invariant factors* of M.
(Side remark: The number n is often called the *Betti number* of M.)

Know the "Compatible Basis Theorem": If N is a submodule of a finitely generated free R-module M (R a PID), then there exist an R-basis $y_1, \dots, y_n$ of M and elements $d_i \in R \setminus \{0\}$ $(1 \leq i \leq s)$, up to multiplication with units uniquely determined by M and N and called the *invariant factors of* N with respect to M, such that $d_1 \mid d_2 \dots \mid d_s$ and $d_1 y_1, \dots, d_s y_s$ is an R-basis of N.

Know How to Decompose if R is Euclidean:
(I) Write $M = F/N$ for F free on n generators $\{y_1, \dots, y_n\}$, and choose (not necessarily free) generators $c_{i1}y_1 + \dots c_{in}y_n$, $i = 1, \dots, m$ for N (in other words: $c_{i1}y_1 + \dots c_{in}y_n = 0$ with $i = 1, \dots, m$ is a set of defining relations for M). Define the *relations matrix* $C = (c_{ij})$.
(II) Now apply elementary row and column operations operations to C until you reach a diagonal form $\mathrm{diag}(d_1, \dots, d_s)$ with $d_i \in R \setminus \{0\}$ and $d_1 \mid d_2 \mid \dots \mid d_s$, meaning that the resulting matrix has $d_1, \dots, d_s$ as its first s entries on the main diagonal and zeros everywhere else (the Euclidean Algorithm guarantees that this is possible).
(III) Then the d_i's which are no units are the invariant factors of M, and M is isomorphic to $\bigoplus_{d_i \notin R^*} R/(d_i) \oplus R^{n-s}$. Keeping track of the column operations, this procedure also yields compatible bases for M and N, implying that $d_1, \dots, d_s$ (including the units) are the invariant factors of N with respect to F.

Related Problems

1. (Sep 82 #2) If $a_1, \dots, a_n$ in a PID R have gcd d, show that there exists an invertible $n \times n$ matrix Q of determinant 1 over R with $Q\,[a_1, \dots, a_n]^T = [d, 0, 0 \dots 0]^T$. (This is false if R is merely a UFD).

2. (Sep 84 #5) If A, B, C are submodules of a general R-module M, with $A \supseteq C$, show $A \cap (B + C) = (A \cap B) + C$.

3. (Sep 84 #6) Find the invariant factors of the following 3×3 matrices over $\mathbb{Z}$, and decide if they are equivalent: $\begin{pmatrix} 10 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{pmatrix}$, $\begin{pmatrix} 4 & 6 & 4 \\ 4 & 20 & 12 \\ 20 & 0 & 20 \end{pmatrix}$.

4. (Sept 86 #5) If M is an artinian module over a general R, show that any injective endomorphism is surjective.
(A module M over a general ring R is called *artinian* if there is no infinite chain of strictly decreasing submodules of M. Standard example (explain why this is an example!): $R =$ finite dimensional K-algebra for a field K and $M =$ finitely generated R-module.)

5. (Jan 87 #6; Aug 88 #6) If I is an ideal of a commutative ring R, show
(a) R/I is simple as an R-module $\iff$ I is a maximal ideal,
(b) I prime $\implies$ R/I is an indecomposable R-module;
(An R-module is called *indecomposable* if it cannot be written as the direct sum of two nonzero R-modules.)
(c) if I is prime, what kind of *ring* is R/I?

6. (May 91 #6) Let $M = \mathbb{Z} \oplus \mathbb{Z}$ be the free module of rank 2 over the ring $\mathbb{Z}$ of integers. Let S be the submodule of M spanned by $x = (3, 0),\ y = (0, 4),\ z = (6, 2)$. Find a $\mathbb{Z}$-basis for the submodule S.

7. (Aug 94 #8) If the *annihilator* of a left R-module M is $Ann_R(M) = \{a \in R \mid aM = 0\}$, show that for submodules M_1, M_2 of M we have $Ann_R(M_1 + M_2) = Ann_R(M_1) \cap Ann_R(M_2)$. Show furthermore that we have $Ann_R(M_1) + Ann_R(M_2) \subseteq Ann_R(M_1 \cap M_2)$, but show that this inclusion could be strict.
Additional question: Is $Ann_R(M_1) + Ann_R(M_2) = Ann_R(M_1 \cap M_2)$ true if R is a PID and M is a finitely generated torsion R-module (no free summand)?

8. (Aug 96 #3) Let M be a finitely generated module over a ring R. Show that *any* generating set for M as R-module must contain a *finite* generating set. Conclude that M has a minimal generating set (no proper subset generates M), and that every minimal generating set of M is finite.

9. (Aug 97 #7) Let M be the free module over $\mathbb{Q}[x]$ with basis v_1, v_2, v_3, N a submodule with basis w_1, w_2, w_3, where

$$\begin{aligned} w_1 &= (x^3 - x^2 - x + 1)v_1 + (2x^2 + 2x)v_2 + (x^3 + x^2)v_3, \\ w_2 &= (2x^3 - 3x^2 - 3x + 2)v_1 + (5x^2 + 5x)v_2 + (2x^3 + 2x^2)v_3, \\ w_3 &= (x^3 - x)v_1 + (x^2 + x)v_2 + (x^3 + x^2)v_3. \end{aligned}$$

(a) There is a theorem which implies that M has another basis u_1, u_2, u_3 for which d_1u_1, d_2u_2, d_3u_3 are a basis for N for some $d_1, d_2, d_3 \in \mathbb{Q}[x]$ such that $d_1 \mid d_2 \mid d_3$. Write a carefully worded statement of this theorem, giving all appropriate hypotheses and conclusions.
(b) Find the values d_1, d_2, d_3 for the example given here.

10. (Jan 98 #4) Let M be a module over a ring. A *section* $A : B$ of M is a pair of submodules A, B of M with $B \subseteq A$; a *trivial section* is where $B = A$. A submodule C of M *covers* a section $A : B$ if $(A \cap C) + B = A$, and *avoids* $A : B$ if $A \cap C \subseteq B$.
(a) Show that C covers $A : B$ iff $A \subseteq B + C$, and avoids $A : B$ iff $A \cap (B + C) = B$.
(b) Show that every C simultaneously covers and avoids any trivial section; that any C with $C \supseteq A$ covers $A : B$; and that any C with $C \subseteq B$ avoids $A : B$.
(c) Give an example of a $\mathbb{Z}$-module M and a submodule C that covers one nontrivial section $A : B$ and avoids another nontrivial section $A' : B'$ for which the two quotients A/B and A'/B' are isomorphic.

11. (Jan 05 #3) Let R be a PID, p a prime element of R and $M \neq \{0\}$ a finitely generated R-module such that there exists a natural number k with $p^kM = \{0\}$. We choose k minimal

with this property, i.e. $p^{k-1}M \neq \{0\}$.
(a) Describe the structure of M. Show that p^k is an elementary divisor of M and that each elementary divisor of M divides p^k.
(b) Let m be any element of M with the property that $p^{k-1}m \neq 0$. Show that the cyclic module $N := Rm$ has a complement C in M, i.e. $M = N \oplus C$.

12. (Jan 08 #2) (a) Let R be a commutative ring with 1, and M a finite direct sum $M = M_1 \oplus \cdots \oplus M_n$ of simple unital left R-modules M_i. Show that M has both the ascending and descending chain conditions on R-submodules.
(b) Where does your argument use the hypotheses that R is unital, R is commutative, or M is unital?

13. (Aug 11 #3) (a) Let V be an noetherian module for a ring R, so that V satisfies the ascending chain condition on submodules. Let $T : V \to V$ be a surjective R-endomorphism. Prove that T is an isomorphism.
(b) In (a) suppose that R is a field, so V is a vector space. Give another explanation of (a) in terms of the rank and nullity of T.

14. (Jan 12 # 6) Let R be a commutative ring with 1. Recall that a left R-module M is called Noetherian if it satisfies the ascending chain condition on submodules and Artinian if it satisfies the descending chain condition on submodules. Assume that an R-module M is both Artinian and Noetherian. (For example, R might be a field, and M might be a finite-dimensional vector space over R). Let $T : M \to M$ be an R-module homomorphism.
(a) Prove that there exists $k \in \mathbb{N}$ s.t. $\mathrm{Ker}(T^k) = \mathrm{Ker}(T^{2k})$ and $\mathrm{Im}(T^k) = \mathrm{Im}(T^{2k})$.
(b) Prove that if k is as in part (a), then $M = \mathrm{Ker}(T^k) \oplus \mathrm{Im}(T^k)$.
(c) Deduce from (a) and (b) that there exist submodules M_0 and M_1 of M s.t. $M = M_0 \oplus M_1$, $T_{|M_0}$ is nilpotent and $T_{|M_1}$ is invertible (as a map from M_1 to M_1).
(d) Now assume that R is a field of characteristic zero, M is a finite-dimensional vector space over R and $\mathrm{tr}(T^n) = 0$ for every $n \in \mathbb{Z}_{>0}$. Prove that T is nilpotent. Hint: Apply (c), assume that $M_1 \neq 0$ and reach a contradiction by applying the Cayley-Hamilton theorem to $T_{|M_1}$.

15. (Aug 15 #5) Let R be a commutative ring with identity, and let I be a nilpotent ideal, i.e., $I^k = 0$ for some k. Let M, N be two R-modules, and let $f : M \to N$ be an R-homomorphism. Suppose that the induced homomorphism from M/IM to N/IN is surjective. Prove that f is surjective.

16. (Jan 16 #3) Let R *be* a commutative ring with identity. A non-zero R-module M is said to be irreducible if 0 and M are the only submodules of M. Prove that M is irreducible if and only if $M \cong R/m$, where m is a maximal ideal of R.

17. (Aug 16 # 7)
(a)Give a complete and irredundant list of abelian groups of order 144.
(b)Give a complete and irredundant list of finitely generated modules over $\mathbb{F}_2[t]$ where the polynomial $t^4 + t^3 + t + 1$ acts trivially.

18. (Jan 17 #7) Consider the matrix

$$A = \begin{bmatrix} 12 & 4 & -16 \\ 4 & 3 & -7 \\ 8 & 3 & -11 \end{bmatrix}.$$

(a) Find the characteristic and minimal polynomials of this polynomial and its Jordan normal form.
(b) Consider map $\mathbb{Z}^3 \to \mathbb{Z}^3$ induced by A. Describe the kernel and cokernel of this map as a sum of copies of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

3.2 Rational and Jordan canonical form

$T : V \longrightarrow V$ is a fixed linear transformation on a finite-dimensional vector space V over a field F, A is an $n \times n$ matrix over F, I denotes the identity transformation and I_n the $n \times n$ identity matrix.

KNOW BASIC DEFINITIONS FOR T (analogously for A, interpreted as a linear transformation on $V = F^n$ acting by left multiplication): *characteristic polynomial* ($\chi_T(x) = \det(xI - T)$), *characteristic root* (root of the characteristic polynomial, λ such that $\det(\lambda I - T) = 0$), *minimum polynomial* $\mu_T(x)$ (monic polynomial of smallest degree satisfied by T); *eigenvalue* (scalar $\lambda \in F$ such that $T(v) = \lambda v$ for some vector $0 \neq v \in V$) and *eigenvector* (vector $0 \neq v \in V$ such that $T(v) = \lambda v$ for some $\lambda \in F$); λ-*eigenspace* V_λ ($= \{v \in V \mid T(v) = \lambda v\} = \{$ eigenvectors of T with eigenvalue $\lambda\} \cup \{0\}$); *generalized eigenvector* of order k ($= \{v \in V \mid (T - \lambda I)^k(v) = 0$ but $(T - \lambda I)^{k-1}(v) \neq 0\}$; order 0 means $v = 0$, order 1 means v is a true eigenvector); *generalized* λ- *eigenspace* V^λ (all generalized eigenvectors); *determinant, trace, rank, nullity, Jordan canonical form* JCF; $r \times r$ *Jordan block* $J_r(\lambda)$; *rational canonical form* RCF for a tranformation T or matrix A, invariant factors and companion matrices.

KNOW THE FOLLOWING FACTS:
(1) *eigenvalues = roots of the characteristic polynomial*
($\det(\lambda I - T) = 0 \iff \lambda I - T$ singular, kills some vector $v \neq 0$, $\iff \lambda v = T(v) \iff v$ is an eigenvector with eigenvalue λ);
(2) *minimum polynomial divides all polynomials satisfied by* T (it is the generator of the ideal in $F[x]$ of all polynomials f satisfying $f(T) = 0$);
(3) $V_\lambda = \ker(T - \lambda I)$, $V^\lambda = \bigcup_k \ker(T - \lambda I)^k$.
(4) V becomes a finitely generated module for the PID $F[x]$ via the action $x.v = T(v)$, so $f(x).v := f(T)(v)$; then V^λ is just the $x - \lambda$-torsion submodule, and a Jordan block $J_r(\lambda)$ in JCF corresponds to a cyclic direct summand $F[x]/((x - \lambda)^r)$, in the decomposition of V considered as $F[x]$-module;
(5) every polynomial splits into linear factors over some extension field, for example the algebraic closure of F, so we may have to pass to an extension in order to get enough eigenvalues and eigenvectors;
(6) if $d_1, \ldots, d_s$ are the (monic) invariant factors of A such that $d_1 \mid d_2 \ldots \mid d_s$, then $\mu_A(x) = d_s$ and $\chi_A(x) = d_1 \ldots d_s$ (implying $\chi_A(A) = 0$ (Hamilton-Cayley) and also that $\chi_A(x)$ divides $\mu_A(x)^n$);

(7) the RCF of A is the direct sum (in the sense of matrices) of the s companion matrices of the invariant factors $d_1, \ldots, d_s$ of A.

KNOW CRITERIONS FOR DIAGONALIZABILITY: T is diagonalizable
$\iff V$ has a basis consisting of eigenvectors of T
$\iff V$ is the (necessarily direct) sum of the eigenspaces V_λ
$\iff$ for each eigenvalue λ of T, $\dim_F V_\lambda$ equals the multiplicity of λ as a root of $\chi_T(x)$
$\iff \chi_T(x)$ splits over F and the JCF of T is diagonal
$\iff \mu_T(x)$ is separable and splits over F

KNOW HOW TO FIND $\ker(T)$ (respectively $\ker(T - \lambda I)$):
Gaussian reduction on the system $Tx = 0$, so in particular
$\dim \ker(T) =$ #free parameters = # columns − # leading-one rows $= n - \mathrm{rk}(T)$.

KNOW HOW TO COUNT: If a matrix A has characteristic polynomial $\chi(t) = \prod(t - \lambda_i)^{f_i}$ and minimum polynomial $\mu(t) = \prod(t - \lambda_i)^{e_i}$, then $f_i \geq e_i$; e_i gives the **size of the largest** Jordan λ_i-block, f_i gives the **total sum of the sizes** of all Jordan λ_i-blocks. $\dim \ker(A - \lambda I_n) =$ **number** of Jordan λ-blocks = **number of independent λ-eigenvectors** (exactly one for each Jordan block), $\dim \ker(A - \lambda I_n)^e =$ number of independent generalized λ-eigenvectors of order $\leq e$ (exactly e for each Jordan λ-block of size $\geq e$, but only r for a Jordan λ-block of size $r \leq e$).

Let $T : V \longrightarrow V$ denote a fixed linear transformation on a finite-dimensional vector space V over a field F. We set $n = \dim_F V$ and, for any eigenvalue λ of T, $N_\lambda := T - \lambda I$, $k_e := \dim_F(\ker(N_\lambda^e))$ and $r_e := \mathrm{rk}(N_\lambda^e)\,(= \dim_F(\mathrm{im}(N_\lambda^e))\,)$. We now count as follows:

For a given eigenvalue λ of T, the number $l = l(\lambda)$ of Jordan λ-blocks is

$$l = \dim \ker(T - \lambda I) = k_1 = n - \mathrm{rk}(T - \lambda I) = n - r_1$$

The number $l_e = l_e(\lambda)$ of Jordan λ-blocks of size e is given by the formula

$$l_e = 2k_e - (k_{e-1} + k_{e+1}) = r_{e-1} - 2r_e + r_{e+1}$$

KNOW HOW TO FIND THE JCF AND RCF:
(1) Compute the characteristic polynomial,
(2) factor it into irreducibles $x - \lambda_i$; FIND JCF FOR EACH EIGENVALUE λ_i SEPARATELY;
(3) (for roots of multiplicity $m > 1$ only) compute $k_e = \dim(\ker(N_\lambda^e))$ for $e = 1, 2, \ldots m$ (stop when dimension reaches m; $k_1 = m$ is the condition that there are enough independent ordinary eigenvectors to diagonalize),
(4) $l_e = 2k_e - k_{e-1} - k_{e+1}$.
(5) For the RCF, you have to find the invariant factors of T. If you already know the JCF, you know the elementary divisors and hence the invariant factors. However, it is sometimes more convenient to derive the invariant factors directly, especially when you know the prime factorization of $\chi_T(x)$ *in* $F[x]$, but not necessarily its roots. For instance, you can then test for which divisors f of $\chi_T(x)$ you get $f(T) = 0$ in order to determine the minimal polynomial $\mu_T(x)$.

REMARKS ON HOW TO FIND A JORDAN BASIS:
(1) This usually involves awkward computations and is therefore not a suitable part of exam

problems. It's different if the given set-up enables you to find a Jordan basis by applying some smart idea instead of boring calculations, e.g. in Problems 17. and 53. below.
Anyhow, the following remarks are sufficient in order to find Jordan bases for "small" matrices $A \in M_n(F)$ (or equivalently: $P \in GL_n(F)$ such that $P^{-1}AP$ is in JCF).
(2) If A is diagonalizable, just exhibit a basis consisting of eigenvectors, i.e. solve the homogeneous systems of linear equations yielding $\ker(A - \lambda I_n)$ for each eigenvalue λ.
(3) If, for a given eigenvalue λ, there is only one Jordan λ-block, which must then be of size m = multiplicity of the characteristic root λ, then choose v in $\ker(N_\lambda^m) \setminus \ker(N_\lambda^{m-1})$, and set $v_1 = N_\lambda^{m-1}(v), v_2 = N_\lambda^{m-2}(v), \ldots, v_m = v$, which yields a Jordan basis for this λ-block.
(4) If there are exactly two Jordan λ-blocks, and one of them is of size 1, then first choose v in $\ker(N_\lambda^{m-1}) \setminus \ker(N_\lambda^{m-2})$, and set $v_2 = N_\lambda^{m-2}(v), v_3 = N_\lambda^{m-3}(v), \ldots, v_m = v$. Note that in this case $\dim V_\lambda = 2$ and $\langle v_2, \ldots, v_m \rangle_F \cap V_\lambda = Fv_2$. So we may complete the Jordan basis for the λ-blocks by choosing $v_1 \in V_\lambda \setminus Fv_2$.
(5) If there are precisely two Jordan λ-blocks, and both are of size 2, then $\dim_F(V^\lambda) = 4$ and $k_1 = 2 = \dim_F(N_\lambda(V^\lambda))$. Now choose a basis v_1, v_3 of $N_\lambda(V^\lambda)$ and find $v_2, v_4 \in V^\lambda$ such that $v_1 = N_\lambda(v_2)$ and $v_3 = N_\lambda(v_4)$ (the latter amounts to solving inhomogeneous linear equations). It is easily checked that v_1, v_2, v_3, v_4 is now a Jordan basis for the two λ-blocks.

Related Problems

In Problems 1. – 15. below, describe (up to similarity, using JCF or RCF) all $n \times n$ matrices M over a specific field F with given characteristic polynomial $\chi(t)$ and/or minimum polynomial $\mu(t)$.

1. (Jan 79 #5) $n = n, F = F,\ \mu(t) =$ product of distinct linear factors (find JCF, find eigenvalues of any polynomial $f(M)$).
2. (Sep 79 #1) $n = 6, F = \mathbb{C},\ \mu(t) = (t+2)^2(t-1)$ (JCF).
3. (Jan 81 #1) $n = 8, F = \mathbb{C}, \mathbb{R},\ \chi(t) = t^2(t^4-1)(t^2-1)$ (RCF over $\mathbb{R}$, JCF over $\mathbb{C}$).
4. (Jan 82 #1; Jan 79 #1) $n = 6, F = \mathbb{C},\ \chi(t) = (t+2)^4(t-1)^2$ (JCF).
5. (Jan 82 #3) $n = 5, F = \mathbb{C},\ \chi(t) = (t-2)^3(t+7)^2,\ \mu(t) = (t-2)^2(t+7)$ (find trace, determinant, JCF, is it diagonalizable?)
6. (Feb 84 #4) $n = 6, F = \mathbb{Q},\ \mu(t) = (t-1)^2(t^2+1)$ (RCF over $\mathbb{Q}$, JCF over $\mathbb{C}$).
7. (Jan 87 #7) $n = 5, F = \mathbb{C}, \mathbb{R},\ \chi(t) = t^5 - t$ (RCF over $\mathbb{R}$, JCF over $\mathbb{C}$).
8. (Aug 88 #2) $n = 6, F = \mathbb{C}, \mathbb{R},\ \chi(t) = t^6 - t^5 - t^2 + t$ (JCF over $\mathbb{C}$, RCF over $\mathbb{R}$).
9. (Jan 89 #5) $n = 9, F = F,\ \mu(t) = t^2(t-1)^2(t+1)^3$.
10. (May 91 #1ab) $n = 6, F = \mathbb{R},\ \mu(t) = t^4 + t^2$ (RCF over $\mathbb{R}$, JCF over $\mathbb{C}$).
11. (May 92 #4) $n = 6, F = \mathbb{C},\ \mu(t) = (t-1)^2(t-2)$ (JCF).

12. (Jan 94 #1) $n = 5, F = \mathbb{Q},\ \mu(t) = (t-2)^2(t+3)$ (find all RCFs; find two such matrices having the same characteristic polynomial but which are still not similar).

13. (Jan 95 #4) $n = 8, F = \mathbb{C},\ \chi(t) = t^8 - t^4,\ \mu(t) = t^6 - t^2$ (JCF).

14. (Aug 95 Comprehensive #6) $n = 10, F = \mathbb{R},\ \mu(t) = (t^4-1)^2$ (find all possible values of k, the maximum number of independent eigenvectors).

15. (Aug 96 #7) $n = 7, F = \mathbb{C}, \mathbb{R},\ \chi(t) = (t-1)^3(t^2+1)^2,\ \mu(t) = (t-1)(t^2+1)^2$ (RCF over $\mathbb{R}$, $\mathbb{C}$, JCF over $\mathbb{C}$).

16. (April 77 #1) Use JCF to show $\det(e^M) = e^{trace(M)}$ for any $n \times n$ complex matrix; find e^M for $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

17. (Nov 77 #6) Let V be the real vector space of all polynomials over $\mathbb{R}$ of degree $< n$ and $T = d/dx$ the linear operator on V defined by differentiating. Determine the JCF of T and exhibit a Jordan basis for T.

18. (May 78 #7) Find inverse of $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

19. (May 78 #8) $F = \mathbb{C}:\ M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$ (find $\chi(t), \mu(t)$, eigenvalues, JCF).

20. (Sep 78 #1) Show that the set of 3×3 rational matrices commuting with $M = \begin{pmatrix} 0 & 0 & 6 \\ 1 & 0 & 4 \\ 0 & 1 & 2 \end{pmatrix}$ form a field.

21. (Sep 78 #2) $n = 12, F = GF(3),\ \chi(t) =$ product of linear factors; find JCF given rank(M) = 10, rank(M^2) = 9, rank(M^3) = 9, rank($M-1$) = 12, rank($M-2$) = 9, rank(($M-2)^2$) = 7, rank(($M-2)^3$) = 6.

22. (May 80 #3) $F = \mathbb{C}:\ M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},\ M_2 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ (find JCF and eigenvalues).

23. (Sep 80 #3) $n = 4, F = \mathbb{C}$, satisfies $f(t) = t^2 - 7t + 10$, trace 11 (find determinant, JCF).

24. (Sep 82 #7) Show two idempotent $n \times n$ matrices are similar iff they are equivalent.

25. (Sep 82 #8) Give two complex 4×4 matrices that have the same minimum and characteristic polynomials, yet are not similar.

26. (Sep 83 #5) If M is any 3×3 real matrix with characteristic polynomial $x^3 + ax^2 + bx + c$, define its adjoint to be $M^* := M^2 + aM + bI$ and show $M^* = \det(M)M^{-1}$ when M is invertible; show $(M^*)^* = \det(M)M$ for any M.

27. (Sep 83 #6) $F = \mathbb{C}:\ M_1 = \begin{pmatrix} 0 & -1 & -1 & -1 \\ 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & -1 & 0 & -1 \\ 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$ (find RCF and JCF).

28. (Sep 84 #4) $F = \mathbb{R}, \mathbb{C}:\ D = d/dx$ on $V = span\{x\sin(x), x\cos(x), \sin(x), \cos(x)\}$ (find $\chi(t), \mu(t)$,invariant factors, RCF over $\mathbb{R}$, JCF over $\mathbb{C}$).

29. (Sep 84 #8) Find the determinant and inverse of the $n \times n$ real matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 2 & 2 & \dots & 2 \\ 1 & 2 & 3 & 3 & \dots & 3 \\ 1 & 2 & 3 & 4 & \dots & 4 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 2 & 3 & 4 & \dots & n \end{pmatrix}.$$

30. (1985 #2) $F = \mathbb{R}:\ M = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$ (find $\chi(t), \mu(t)$, JCF).

31. (Sep 86 #3) Show that linear operators S, T on a finite-dimensional V are similar if
(i) $\text{rank}(S^m) = \text{rank}(T^m)$ for all $m = 0, 1, \dots$, and
(ii) $S^n = 0$ for some n.

32. (Fall 87 #6) Find RCF of the 9×9 matrix over $\mathbb{R}$ whose JCF is
$M = Diag\{J_2(2), J_1(2), J_2(2), J_2(i), J_2(-i)\}$.

33. (May 89 #1) $F = \mathbb{C}:\ M = \begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}$ (find RCF and JCF).

34. (May 89 #9) If an $n \times n$ matrix M over F has an elementary divisor $\lambda - a$ ($a \in F$) show there is an invertible $n \times n$ matrix Q over F with $Q^{-1}MQ = \text{RCF}(M)$ AND $\det(Q) = 1$.

35. (Aug 89 #7) $n = 2, F = GF(2)$, ALL POSSIBLE RCFs.

36. (May 1990 #7) Explain which of these 8×8 matrices are similar.

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & -3 & 0 & -3 & 0 \end{pmatrix}, \; M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -i & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -i & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i \end{pmatrix},$$

$$M_3 = \begin{pmatrix} i & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & i & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -i & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

37. (May 91 #1c) Suppose M has the property that $trace(M^k) = 0$ for all $k > 0$, and that its minimum polynomial divides $t^4 + t^2$. Show that M is nilpotent.
(Imprecise formulation of the problem; assume $M \in M_n(F)$ and $\text{char}(F) = 0$ or $\text{char}(F) > n$.)

38. (Jan 92 #5) $n = n, F = F$, satisfies $f(t) = t^2 - t$ (is *idempotent*, $M^2 = M$) (show two such are similar iff they have the same rank).

39. (May 92 #7) If a real 2×2 symmetric matrix M has $\lim_{k\to\infty} trace(M^k) = 0$, show $\lim_{k\to\infty} M^k = 0$ too. Does this hold for $n \times n$ real symmetric matrices?

40. (Sep 93 #1) $n = n, F = \mathbb{R}$, satisfies $f(t) = t^3 - t$ (is *tripotent*, $M^3 = M$) (show two such are similar iff they have the same rank and the same trace).

41. (Aug 94 #4b) $n = n, F = \mathbb{C}$, satisfies $f(t) = t^d - 1$ (has order d, smallest positive exponent such that $M^d = I$) (JCF).

42. (Aug 95 #4) If T is a diagonalizable linear operator on a finite-dimensional vector space V and W is a T-invariant subspace of V, prove W has a T-invariant complement (a subspace U such that $V = W \oplus U$).

43. (Aug 95 #5) $F = \mathbb{R}: \; M = (a_{ij})$ with $a_{ij} = 1$ for $i \le j$ and $a_{ij} = 0$ for $i > j$ (find JCF).

44. (Jan 97 #1) $F = \mathbb{R}, \mathbb{C}: \; M = \begin{pmatrix} -1 & 3 & 0 \\ 0 & 2 & 0 \\ 2 & 1 & -1 \end{pmatrix}$ (find RCF over $\mathbb{R}$, JCF over $\mathbb{C}$).

45. (Aug 97 #1b) Let K be a field containing n distinct n-th roots of unity, L an extension field such that $Gal(L/K)$ is a cyclic group of order n with generator σ. Find the Jordan canonical form of σ.
Hint: It is proved in field theory (and you may use this here) that L must be of the form

$L = K(\sqrt[n]{a})$ for some $a \in K$.
Additional question: If T denotes multiplication by $\sqrt[n]{a}$, considered as a K-linear transformation of L, what is the RCF of T (over K) and what is the JCF of T (over L)?

46. (Jan 98 #7) If the $n \times n$ real matrix P is the transition matrix for a regular Markov chain, then its powers converge to a matrix $T = \lim_{k\to\infty} P^k$ of the form $\begin{pmatrix} t_1 & t_1 & \dots & t_1 \\ t_2 & t_2 & \dots & t_2 \\ \dots & \dots & \dots & \dots \\ t_n & t_n & \dots & t_n \end{pmatrix}$ all of whose columns are the same probability vector $\vec{t}$ (its entries t_i are all nonnegative and sum to 1).
(a) What is the JCF of the limit T?
(b) What are the possible complex eigenvalues of the original P?
(c) What are the possible JCFs of P? If you cannot do the general case, do at least the 2×2 case.

47. (Aug 98 #6) Let V be an n-dimensional vector space over the complex numbers, and let T be a linear transformation from V to itself whose minimum polynomial $\mu(x)$ has degree 2.
(a) Find all possible Jordan Canonical Forms for T. (*Hint:* consider the possible factorizations of $\mu(x)$ over K.)
(b) Show that V is a direct sum of T-invariant subspaces, each of which has dimension less than or equal to 2.
(c) Show that T has an eigenvalue λ such that the λ -eigenspace (the set of all eigenvectors for the eigenvalue λ, together with the zero vector) has dimension at least $n/2$.

48. (Aug 99 #6) Describe (in terms of Jordan form) all 2×2 complex matrices which are similar to their square. (*Hint:* There are more matrices, Horatio, than are dreamt of in your philosophy!)

49. (Aug 99 #7) (a) Show that the ring of $2n \times 2n$ matrices $M_{2n}(F)$ over a field F for $n \geq 1$ is "algebraically closed" with respect to polynomials of degree 2, in the sense that every polynomial $p(x) = x^2 + \alpha x + \beta \in F[x]$ of degree 2 has a "root" $A \in M_{2n}(F)$ (in the sense that $p(A)$ is the zero matrix). Can you generalize this to polynomials of degree d?
(b) How many real 2×2 matrices $A \in M_2(\mathbb{R})$ are the roots of the polynomial $p(x) = x^2 + 1$?

50. (Aug 01 #5) How many non-similar linear transformations T can there be on an 8-dimensional real vector space V having the minimum polynomial $\mu_T(t) = (t-2)(t-3)(t-6)^3$? *List* their Jordan canonical forms.

51. (Aug 01 #6) Consider the linear transformation T on $\mathbb{R}^3$ which rotates points around the z-axis through a fixed angle θ.
(a) Find the matrix of T with respect to the canonical basis for $\mathbb{R}^3$.
(b) Find the characteristic polynomial of T, and factor it into irreducibles (ignore the cases when θ is an integer multiple of π).
(c) Find the Jordan canonical form for T (you may have to pass to complex matrices).

52. (Aug 02 #2) Show that if for a matrix $A \in M_n(K)$ (where K is a field) there exists a nonzero matrix $B \in M_n(K)$ such that $AB = 0$, then there also exists a nonzero matrix $C \in M_n(K)$

such that $CA = 0$ (in other words, in $M_n(K)$ the set of *left* zero divisors coincides with the set of *right* zero divisors; note that $AB = 0$ does **not** always imply $BA = 0$ - find such examples!)

53. (Aug 03 #3) Let P_{2n-1} be the vector space of polynomials in one variable x with real coefficients of degree $\leq 2n-1$. Let T denote the linear operator on P_{2n-1} defined by $p(x) \mapsto p(x) + p''(x)$ for every $p(x) \in P_{2n-1}$, where p'' denotes the second derivative.
(a)Determine the matrix A_T of the operator T with respect to the basis $\{1, x, x^2, \ldots, x^{2n-1}\}$.
(b) Find the Jordan canonical form of A_T AND a Jordan basis for T.

54. (Jan 04 #3) Let $A, B \in M_n(\mathbb{C})$ be two commuting matrices. Prove that they have a common eigenvector in $\mathbb{C}^n$, i.e. there exists a nonzero $v \in \mathbb{C}^n$ such that $Av = \lambda v$ and $Bv = \mu v$ for some $\lambda, \mu \in \mathbb{C}$.

55. (Jan 04 #6) Prove:
(a) If $A \in M_n(\mathbb{R})$ is idempotent, then it is diagonalizable.
(b) Two idempotent matrices $A, B \in M_n(\mathbb{R})$ are similar if and only if they have the same rank.

56. (Aug 04 #6) Let K be an arbitrary field ($\rightarrow$ case distinction!). Classify, up to similarity, all matrices $A \in GL_4(K)$ of order 2. (Use an appropriate canonical form.)

57. (Aug 04 #7) Consider the group $G = SL_2(\mathbb{F}_4)$.
(a) (4 points) Show *without* specifying any matrix that G contains an element of order 5.
(b) (8 points) Exhibit a concrete matrix $A \in SL_2(\mathbb{F}_4)$ of order 5. Use $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where α is a root of $x^2 + x + 1$. Describe in detail how you obtained A; you shouldn't just guess! (Hint: You might first factorize $x^5 - 1$ in $\mathbb{F}_4[x]$.)

58. (Jan 05 #7) Let $A = (a_{ij}) \in M_n(\mathbb{Q})$ be given by $a_{ii} = 0$ for all i and $a_{ij} = 2$ for all $i \neq j$. Determine the Jordan canonical form of A.

59. (Aug 05 #6) Let $A = J_n(\lambda) \in M_n(\mathbb{C})$ be a Jordan λ-block ($\lambda \in \mathbb{C}$).
(a) Determine $\dim_{\mathbb{C}} \mathbb{C}[A]$.
(b) For $\lambda \neq 0$ and any natural number k, determine the Jordan canonical form of A^k.
Include arguments for both parts!

60. (Aug 05 #7) Show that there does *not* exist any matrix $A \in M_{10}(\mathbb{Q})$ satisfying $A^4 = -I_{10}$.

61. (Jan 06 #5 and #6) V is a finite-dimensional F-vector space, F a field and $T : V \rightarrow V$ a linear transformation.
(5) Let $T = \lambda Id + Z$ for λ in a field F of characteristic 0 and Z nilpotent. Show that if $T^k = Id$ for some $k > 0$ then Z must be the zero transformation.
(6) If $T(v) \in Fv$ for all $v \in V$, show that $T = \lambda Id$ is a "scalar" for some $\lambda \in F$.

62. (Jan 06 #7) Prove: If G is a finite subgroup of $SL_2(\mathbb{C})$ then $Av = v$ for $A \in G$, $v \in \mathbb{C}^2$ implies $A = I_2$ or $v = 0$.

63. (Aug 06 #6) Over $\mathbb{C}$, find the RCF, JCF, the elementary divisors, the invariant factors, the characteristic and the minimal polynomial of:

$$\begin{pmatrix} 0 & -1 & 3 \\ 1 & 2 & -3 \\ 1 & 1 & -2 \end{pmatrix}$$

64. (Jan 08 #3) Let V be an n-dimensional vector space V over a finite field F of q elements.

(a) Show that the number of invertible linear operators on V is $\prod_{i=0}^{n-1}(q^n - q^i)$.

(b) Find the cardinality $|P|$ of any 3-Sylow subgroup $P \leq G = \mathrm{GL}(4, \mathbb{F}_{81})$ where $n = 4$ and $F = \mathbb{F}_{81}$ is the field of $q = 81$ elements.

$|P| =$ $\boxed{}$

(c) Find the cardinality $|P'|$ of any 3-Sylow subgroup $P' \leq G'$ of the special linear group $G' = \mathrm{SL}(4, \mathbb{F}_{81})$ (those invertible 4×4 matrices of determinant 1) over a field $\mathbb{F}_{81}$ elements.

$|P'| =$ $\boxed{}$

(d) Describe up to similarity (in terms of Jordan canonical forms) all possible 3-torsion elements T of the general linear group $\mathrm{GL}(4, \mathbb{F}_{81})$: all invertible operators T with $T^{3^e} = Id$ for some $e \geq 0$. For each T list its minimum polynomial $\mu_T(x)$ and its 3-period (the smallest $e \geq 0$ with $T^{3^e} = Id$). [Hint: all eigenvalues of T already lie in $\mathbb{F}_3$.]

65. (Aug 08 #1) Let A be the 5-by-5 real matrix $\mathrm{A} := \begin{bmatrix} 2 & 1 & 4 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}$

a. What is the characteristic polynomial $\chi_A(x)$ and the minimal polynomial $\mu_A(x)$?

b. Up to similarity, how many matrices $B \in \mathbb{M}_{5\times 5}(\mathbb{R})$ have the same characteristic polynomial $\chi_B(x) = \chi_A(x)$?

c. What is the Jordan Canonical Form of A?

66. (Jan 09 #5) Let F be an algebraically closed field, and let $M_n(F)$ be the ring of $n \times n$ matrices over F.

(a) Prove that for any $A \in M_n(F)$ the centralizer of A has dimension at least n. (Hint: look

at each Jordan block.)
(b) Describe all matrices $A \in M_n(F)$ with the property that every matrix commuting with A is diagonalizable.

67. (Aug 09 #5) (a) Let $A = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 4 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{C})$. Find the minimal polynomial, the characteristic polynomial and the Jordan canonical form of A.
(b) Let $J_n(0) \in M_n(\mathbb{C})$ be the Jordan block of size $n \geq 2$ with 0's on the diagonal. Prove that there exists no matrix $A \in M_n(\mathbb{C})$ such that $A^2 = J_n(0)$.

68. (Aug 10 #5) Let F be a field, $M_2(F)$ the ring of 2×2 matrices over F and $GL_2(F)$ the group of invertible elements of $M_2(F)$.
(a) Prove that two matrices in $M_2(F)$ are similar if and only if they have the same minimal polynomial.
(b) Assume that F is finite, and let $q = |F|$. Find the number of conjugacy classes in $GL_2(F)$.
(c) Again assume that F is finite of order q. Find the number of nilpotent matrices in $M_2(F)$.
Hint: If $A \in M_2(F)$ is nilpotent, what is its Jordan normal form? You may use without proof that $|GL_2(F)| = (q^2 - 1)(q^2 - q)$.

69. (Aug 11 #5) This problem tests some standard linear algebra facts. You can quote standard theorems.
Let F be a field and let $T : F^6 \to F^6$ be a linear operator with characteristic polynomial $\chi_T(t) = (t^2 + t + 1)(t^2 - 1)t^2$.
(a) If $F = \mathbb{R}$, what are the various possibilities for the minimal polynomial $\mu_T(t)$ of T?
(b) Determine $\det(T)$ and $\text{trace}(T)$. Be careful about signs!
(c) Write down the companion matrix C of the polynomial $\chi_T(t)$. Calculate the minimal polynomial of C.
(d) When $F = \mathbb{C}$, when is T diagonalizable (i.e., represented by a diagonal matrix w.r.t. some basis)? Some explanation in terms of $\chi_T(t)$ or $\mu_T(t)$ is required.
(e) When $F = \mathbb{R}$, when (if ever) is T represented by a symmetric matrix? Why?
(f) Bonus: Let $S : \mathbb{C}^m \to \mathbb{C}^m$ be a nilpotent operator which is represented by a matrix in Jordan normal form having blocks of sizes $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1$. Let $\lambda' = (\lambda'_1, \ldots, \lambda'_s)$ be the partition of m dual (or transpose) to the partition $\lambda = (\lambda_1, \ldots, \lambda_r)$ of m. What is the significance (in terms of S) of the integers λ'_i, $i = 1, \ldots, s$? (Note: your answer should be precisely one [short] sentence! No further explanation is wanted.)

70. (Jan 12 # 5) Let F be a field, n a positive integer and $M_n(F)$ the set of $n \times n$ matrices over F. Let $A \in M_n(F)$ be such that $A^2 = A$. Prove that A is diagonalizable and classify all such A up to similarity. (Recall that $A, B \in M_n(F)$ are similar if there exists $C \in GL_n(F)$ s.t. $C^{-1}AC = B$.)

71. (Aug 12 #6) Let p be an odd prime number and n an integer ≥ 2.

    (a) Show that $GL_n(\mathbb{Q})$ has an element of order p if and only if $n \geq p - 1$.

    (b) Show that there is an $A \in GL_n(\mathbb{Q})$ of order p which does NOT have 1 as an eigenvalue if and only if $p - 1$ divides n.

(c) Let $A \in GL_4(\mathbb{Q})$ be an element of order 5. Prove that the complex JCF of A is independent of such A (up to permutation of blocks) and write it down.

72. (Jan 13 #6) Let F be an algebraically closed field and $A \in Mat_n(F)$ an $n \times n$ matrix over F for some $n \geq 2$.

(a) Prove that there exist a diagonalizable matrix D and a nilpotent matrix N (that is, $N^k = 0$ for some $k \in \mathbb{N}$) such that $A = D + N$ and D and N commute, that is, $DN = ND$.

(b) Assume that A itself is diagonalizable. Prove that if D and N satisfy the conditions of part (a), then $N = 0$ (and hence $D = A$). **Hint:** You may use the following fact without proof: if two diagonalizable matrices X and Y commute, then they are simultaneously diagonalizable, that is, there exists an invertible matrix Q such that $Q^{-1}XQ$ and $Q^{-1}YQ$ are both diagonal.

73. (Aug 13 #4) Let K be a field, and let $M_n(K)$ be the ring of $n \times n$ matrices with entries in K. For this problem, let $D \in M_n(K)$ be diagonalizable (over K) and, for each eigenvalue λ of D, let

$$E_\lambda := \{v \in K^n \mid Dv = \lambda v\}$$

be the corresponding eigenspace.

(a) For any $A \in M_n(K)$, show that $AD = DA$ if and only if $A(E_\lambda) \subseteq E_\lambda$ for all eigenvalues λ of D.
(Hint: For the "if" part, you may use that $AD = DA$ if $ADv = DAv$ for all $v \in K^n$.)

(b) If A is also diagonalizable and $AD = DA$, show that A and D are simultaneously diagonalizable (that is, there is a matrix P such that both PAP^{-1} and PDP^{-1} are diagonal). Provide a counter-example showing that this need not be the case if the matrices do not commute.

(c) If D is invertible, show that the centralizer of D in $GL_n(K)$ is isomorphic to a direct product $GL_{n_1}(K) \times \ldots \times GL_{n_r}(K)$, where $n_1 + \ldots + n_r = n$. Also show that each of these products can be realized as the centralizer of some (appropriately chosen) D, provided that K has at least $n + 1$ elements.

74. (Jan 14 #1) Let K be an algebraically closed field of characteristic 0. Show that any element of finite order in $GL_n(K)$ is diagonalizable. (Hint: Jordan Form!).

75. (Aug 14 #4) Denote by J the $n \times n$ Jordan block with eigenvalue 0. For a positive integer k, determine the Jordan canonical form of J^k. (Hint: you can start by playing with some small values of k).

76. (Aug 15 #4) Find the characteristic polynomial, the minimal polynomial, and the Jordan canonical form of the matrix (over the complex numbers)

$$A = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}.$$

77. (Aug 15 #6) Let F be a field and A an n by n matrix with coefficients in F. Assume that A has only one invariant factor. Prove that for every n by n matrix B with coefficients in F such that $AB = BA$ there is a polynomial $p(t) \in F[t]$ such that $p(A) = B$. (Hint: consider the structure of $V = F^n$ as an $F[A]$-module. Use that an endomorphism is determined by its action on a basis.)

78. (Jan 16 # 5) Let T be a linear operator on a finite dimensional vector space V over a field F. Prove that
$$rank(T^3) + rank(T) \geq 2 \cdot rank(T^2).$$

79. (Jan 16 #9) Let
$$A = \begin{pmatrix} 5 & 4 & 3 \\ -1 & 0 & -3 \\ 1 & -2 & 1 \end{pmatrix}.$$
Think of A as a matrix over the complex numbers. Find a 3 by 3 invertible matrix P such that $P^{-1}AP$ is in Jordan canonical form.

80. (Aug 16 # 1) Consider the 3×3 matrix with entries in $\mathbb{Q}$
$$A = \begin{bmatrix} 0 & -2 & 1 \\ 1 & 2 & -1 \\ 3 & -1 & -3 \end{bmatrix}$$
(a) Describe a field extension F of $\mathbb{Q}$ of minimal degree (either abstractly, or as a subfield of the complex numbers), such that A has an eigenvector with entries in F (note: you do **not** need to find the eigenvector or eigenvalue).
(b) Determine if A is diagonalizable over $\mathbb{C}$.
(c) Does there exist a 3×3 matrix with rational coefficients with no eigenvectors over $\mathbb{Q}$ which is not diagonalizable over $\mathbb{C}$? Find a counterexample, or prove none exists.

81. (Aug 16 # 8) Let $n > 1$ and $m > 1$ be natural numbers, and c a complex number. Consider the associated $n \times n$ Jordan block
$$J_n(c) = \begin{bmatrix} c & 1 & 0 & \cdots & 0 \\ 0 & c & 1 & \cdots & 0 \\ 0 & 0 & c & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & c \end{bmatrix}$$
(a) Show that $J_n(c)$ is an m-th power (i.e., there exists B such that $J_n(c) = B^m$) if and only if $c \neq 0$.
(b) Show that any element of $GL_n(\mathbb{C})$ is an mth power.

82. (Aug 17 #3) Let p be a prime, n a natural number and $A \in GL_n(\mathbb{F}_p)$ diagonalizable over the algebraic closure $\overline{\mathbb{F}_p}$.
(a) (4 points) Show that the order of A in $GL_n(\mathbb{F}_p)$ is equal to the lcm of the orders of the eigenvalues of A in $\overline{\mathbb{F}_p}^{\times}$.

(b) (8 points) Prove that $GL_n(\mathbb{F}_p)$ has an element of order $p^n - 1$ which is diagonalizable over $\overline{\mathbb{F}_p}$.
(c) (4 points) Explicitly construct an element of order 8 of $GL_2(\mathbb{F}_3)$.

83. (Aug 17 #8) Consider the $\mathbb{C}$-vector space $V = M_2(\mathbb{C})$ of complex 2×2 matrices and the linear transformation $T : V \longrightarrow V$ defined by $T(X) = AX - XA$ for all $X \in M_2(\mathbb{C})$, where A is the matrix $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Determine (as a 4×4 matrix) the Jordan canonical form of T.

84. (Jan 18 #5) We set $M := M_3(\mathbb{Q})$ and denote by 0 the zero matrix and by I the identity matrix of M.
(a) (2 points) Prove or disprove: If $A \in M$ satisfies $A^6 = 0$, then also $A^3 = 0$.
(b) (4 points) Classify, up to similarity, all matrices in M satisfying $A^6 = 0$. Exhibit one representative for each such similarity class.
(c) (2 points) Prove or disprove: If $A \in M$ satisfies $A^6 = I$, then also $A^3 = I$.
(d) (8 points) Classify, up to similarity, all matrices in M satisfying $A^6 = I$. Exhibit one representative for each such similarity class.

85. (Jan 18 #6) Let $n \geq 2$ be a natural number, F a field and $A = (a_{ij}) \in M_n(F)$ the matrix with entries $a_{ij} = j \cdot 1_F \in F$ for all $1 \leq i, j \leq n$.
Determine the characteristic polynomial, the minimal polynomial and the JCF of A.
Hint: The result may depend on the characteristic of F.

Chapter 4

Some Multilinear Algebra

4.1 Dual spaces and bilinear forms

KNOW THE BASIC DEFINITIONS: *Linear form* (or functional), *dual space* V^* (space of all linear forms), *dual basis* $\mathcal{B}^*$ (to a basis $\mathcal{B}$ for V); *annihilator* (of a subset of V^* in V); dual (or *adjoint* or transpose) $T^* : W^* \to V^*$ of a linear transformation $T : V \to W$ (defined by $T^*(f) = f \circ T$ for $f \in W^*$); *Bilinear form* B on V (bilinear map $V \times V \to F$) *left* and *right duality maps* $B_L, B_R : V \to V^*$ (via $B_L(x) := B(x, \cdot)$, $B_R(x) := B(\cdot, x)$); *symmetric, alternating, skew symmetric, nondegenerate, anisotropic* ($B(x, x) = 0 \Rightarrow x = 0$) bilinear form. *Orthogonal direct sum* $V_1 \perp V_2$, *isometry* $V_1 \to V_2$ of spaces with bilinear forms, *orthogonal* T (isometry $V \to V$). *Symplectic plane* for an alternate bilinear form (basis u, v with $B(u, v) = 1$, hence $B(u, u) = B(v, v) = 0$, $B(v, u) = -1$).

DEFINITIONS FOR A GIVEN BILINEAR FORM B : *Matrix* $Mat_{\mathcal{B}}(B)$ of B relative to an ordered basis $\mathcal{B} = \{x_1, \ldots, x_n\}$ of V ($b_{ij} = B(x_i, x_j)$); *left* and *right annihilators* (or *orthogonal complements*) $U^{\perp,L}$, $U^{\perp,R}$ of a subspace U (the vectors x killing U from the left or right, $B(x, U) = 0$ or $B(U, x) = 0$), *left* and *right radical* $Rad_L(B) = \ker(B_L) = V^{\perp,L}$, $Rad_R(B) = \ker(B_R) = V^{\perp,R}$, *left, right orthogonality, orthosymmetric* ($B(x, y) = 0 \Rightarrow B(y, x) = 0$; standard examples: symmetric and alternating forms). *Isotropic vector* ($B(x, x) = 0$).

KNOW FACTS:
(1) $Bil(V) \cong Hom(V, V^*)$ linear map (L or R) $V \to V^*$ (B gives $L = B_L$, $R = B_R$; L or R gives $B(x, y) = L(x)(y)$ or $B(x, y) = R(y)(x)$);
(2) IF V IS FIN. DIM., nondegenerate bilinear form on $V \cong$ isomorphism (L or R) $V \to V^*$; a bilinear form B is *nondegenerate* $\Leftrightarrow$ *left nondegenerate* (left radical zero) $\Leftrightarrow$ *right nondegenerate* (right radical zero) $\Leftrightarrow$ some/any matrix of B is invertible ($\det(b_{ij}) \neq 0$), $Mat_{\mathcal{B}}(B) = Mat_{\mathcal{B}^*,\mathcal{B}}(B_R) = Mat_{\mathcal{B}^*,\mathcal{B}}(B_L)^t$, $Mat_{\mathcal{B}'}(B) = P^t Mat_{\mathcal{B}}(B) P$ for the *change-of-basis matrix* $P = Mat_{\mathcal{B}',\mathcal{B}}(Id) \Rightarrow$ the *discriminant* $\det(Mat_{\mathcal{B}}(B))(F^*)^2 \in F^*/(F^*)^2 \cup \{0\}$ is a well-defined invariant of B; it is zero iff B is degenerate.

(3) If V is again finite-dimensional and $B : V \times V \to F$ a nondegenerate symmetric bilinear form, we may identify V with V^* via B, i.e. we may identify each $x \in V$ with $B_L(x) = B_R(x) \in V^*$ (since B is symmetric, $B_L = B_R$). Making this identification, any endomorphism of V^* can also be interpreted as an endomorphism of V. Then the dual $T^* : V \to V$ of an endomorphism T of V is characterized by the following property:
$B(x, T(y)) = B(T^*(x), y)$ for all $x, y \in V$.

Basic Splitting Lemma: If B is orthosymmetric, any finite-dimensional nondegenerate subspace U of V is an orthogonal direct summand, $V = U \perp U^{\perp}$.

Basic Structure Theorem:
(I) Any space with **alternating** form is a direct sum $V = P_1 \perp \ldots \perp P_r \perp R$ for R the radical, P_i symplectic planes; thus the rank of V is even and the determinant of any matrix of B is a square.
(II) Any vector space over a field F with $\mathrm{char}(F) \neq 2$ with **symmetric** form is a direct sum $V = L_1 \perp \ldots \perp L_r \perp R$ for R the radical, L_i anisotropic lines (Fu_i with $B(u_i, u_i) \neq 0$); thus there is an orthogonal basis $\{u_1, \ldots, u_r, z_{r+1}, \ldots, z_{r+s}\}$ relative to which B has diagonal matrix. Over an algebraically closed field, we can assume all $B(u_i, u_i) = 1$; over the reals, we can assume all $B(u_i, u_i) = \pm 1$, with the numbers of +1's, -1's, and 0's being invariants of B by *Sylvester's Law of Inertia.*

Related Problems

1. (Aug 94 #5) If $f(x, y)$ is an alternating bilinear form on a 25-dimensional real vector space, and A is its matrix with respect to some basis, show that $\det(A)^{25} = 0$.

2. (Aug 95 #7) Show that every element of $SO_5(\mathbb{R}) = \{A \in GL_5(\mathbb{R}) \mid (Ax, Ay) = (x, y) \text{ and } \det(A) = +1\}$ [where $(x, y) = x \cdot y = x^t y$ is the usual dot product on $\mathbb{R}^5$] has a nonzero fixed point $Ax = x \neq 0$.

3. (Aug 95 #10) It is easy to check that the space $M_n(\mathbb{R})$ of $n \times n$ real matrices is a real inner product space with inner product given by: $\langle A, B \rangle = trace(AB^t)$, where B^t denotes the transpose of the matrix B. Let P be an invertible matrix and T the linear operator on $M_n(\mathbb{R})$ defined by $T(A) = P^t AP$. Denote the adjoint of T relative to this inner product by T^*. Prove that $T^*(A) = PAP^t$ for all A, and find necessary and sufficient conditions on the matrix P that $T = T^*$. Justify your answer.

4. (Jan 97 #7) Let V be a finite-dimensional vector space over a field F, and let λ and μ be two linear functionals on V. Define $B(x, y) = \lambda(x)\mu(y) - \lambda(y)\mu(x)$ for $x, y \in V$. Show that B is an alternating bilinear form on V, and determine the possible values for its rank.

5. (Jan 00 #1) *Define* the trace of an $n \times n$ real matrix, and *show* that the trace of the product XY of two real $n \times n$ matrices is the same as the trace of YX.
   (b) *Explain* why the trace of such a matrix is the *sum of all eigenvalues* (possibly complex, with the appropriate multiplicities) of the matrix.
   (b) *Explain* how you would *define* the trace of an abstract *linear operator* on any finite-dimensional real vector space V (i.e., a linear transformation from V to V).

6. (Jan 00 #2) Let K be a field of characteristic zero, $M_n(K)$ the $n \times n$ matrices over K.
   (a) *Determine* all linear functionals $f : M_n(K) \longrightarrow K$ which are *symmetric* in the sense that $f(ab) = f(ba)$ for all matrices $a, b \in M_n(K)$.
   (b) *Determine* all linear functionals $f : M_n(K) \longrightarrow K$ which are *invariant* in the sense that $f(gag^{-1}) = f(a)$ for all invertible $g \in GL_n(K)$.

7. (Aug 03 #6) Let B be a symmetric bilinear form on a finite-dimensional vector space V over a field F. For a subspace $W \subseteq V$, we define the annihilator subspace of W in V: $W^\perp = \{x \in V \mid B(x, w) = 0 \text{ for every } w \in W\}$. Assume further that B is nondegenerate, that is $V^\perp = \{0\}$. Show that:
   (a) there is a natural isomorphism of vector spaces from $V/W^\perp$ to the dual space W^* of W;
   (b) $\dim W^\perp = \dim V - \dim W$;
   (c) $(W^\perp)^\perp = W$.

4.2 Tensor products (over commutative rings)

KNOW: the defining universal property of tensor products, the fact that tensor products uniquely exist; easy rules for tensor products (commutativity, associativity, $R \otimes_R M = M$, distributivity for direct sums); tensor products of R-linear maps; the fact that injectivity is in general not preserved by tensoring with M; the definition of flat modules ($M \otimes_R$ preserves injectivity nevertheless); the fact that a module is flat if all its finitely generated submodules are flat; the implications "free $\Rightarrow$ projective $\Rightarrow$ flat" for all (commutative) rings; "flat $\Rightarrow$ torsion free" for integral domains; the equivalences "free $\Leftrightarrow$ projective" and "flat $\Leftrightarrow$ torsion free" for PID's; scalar extensions and the general definition of "rank" for an integral domain R: $\mathrm{rk}_R(M) := \dim_F(F \otimes_R M)$ (M an R-module, $F :=$ field of fractions of R).

KNOW THE BASIC LEMMA FOR TENSOR PRODUCTS OF FREE MODULES:
If $\{e_i \mid i \in I\}$ is an R-basis of M and $\{f_j \mid j \in J\}$ is an R-basis of N, then $\{e_i \otimes f_j \mid i \in I \text{ and } j \in J\}$ is an R- basis of $M \otimes_R N$.
Consequence: $\dim(V \otimes_F W) = \dim V \cdot \dim W$ for F-vector spaces V and W.

RELATED PROBLEMS

1. (Aug 03 #4) (a) Determine the following tensor products and explain your answers.
   (i) $\mathbb{R} \bigotimes_{\mathbb{Z}} \mathbb{Z}_{2003}$;
   (ii) $\mathbb{Q}[x]/(x^2+1) \bigotimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^2+2)$.
   (b) Let V and W be finite-dimensional vector spaces over a field F, and $\{v_1, \ldots, v_n\}$ be a basis of V. Prove that if
   $$v_1 \otimes w_1 + \ldots + v_n \otimes w_n = 0$$
   in $V \bigotimes_F W$ for $w_1, \ldots w_n \in W$, then $w_1 = \ldots = w_n = 0$.

2. (Jan 04 #6) Let V and W be finite-dimensional vector spaces over a field k, and let $f : V \to V$ and $g : W \to W$ be linear operators. One can define a linear operator $f \otimes g : V \bigotimes_k W \to V \bigotimes_k W$. Show that $Tr(f \otimes g) = Tr(f) \cdot Tr(g)$.

3. (Aug 04 #8) Let K be a field, V a finite-dimensional vector space over K, and v, w two non-zero vectors in V. Show that $v \otimes w = w \otimes v$ in $V \otimes_K V$ if and *only if* there exists a $c \in K^*$ such that $w = cv$.

4. (Aug 06 #9) Let M/K be a field extension and let $\zeta \in M \setminus K$ be algebraic over K. Let $L := K(\zeta)$ denote the intermediate field generated by ζ. Show that $L \bigotimes_{K[x]} K[[x]] = \{0\}$. Here, we consider L as a $K[x]$-module where we let act x as multiplication by ζ.

5. (Aug 08 #2) Prove the following statements about tensor products.
   (a) $\mathbb{Z}_5[x] \bigotimes_{\mathbb{Z}} \mathbb{Q}[x] = 0$.
   (b) $\mathbb{Q}(i) \bigotimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(i + \sqrt{2})$ as $\mathbb{Q}$-vector spaces.

6. (Jan 09 #8) Let R be a commutative integral domain with 1, and let I be a principal ideal of R. Prove that the R-module $I \bigotimes_R I$ is torsionfree.
   In parts (b) - (d) of this problem let $R = \mathbb{Z}[x]$ and $I = (2, x)$.
   (b) Let $m = 2 \otimes x - x \otimes 2 \in I \bigotimes_R I$. Find a nonzero element $r \in R$ such that $rm = 0$.
   (c) Consider the mapping $\phi : I \times I \to \mathbb{Z}/2\mathbb{Z}$ given by

$$\phi(p(x), q(x)) = \frac{p(0)}{2} q'(0) \mod 2.$$

   where q' is the formal derivative of q. Also consider $\mathbb{Z}/2\mathbb{Z}$ as an R-module via the canonical projection $R \to \mathbb{Z}/2\mathbb{Z}$, i.e. $f.a := f(0)a \bmod 2$ for $f \in R$ and $a \in \mathbb{Z}/2\mathbb{Z}$. Prove that ϕ is R-bilinear.
   (d) Use (c) to prove that $2 \otimes x \neq x \otimes 2$ in $I \bigotimes_R I$ (and thus, by (b) $I \bigotimes_R I$ is not trosionfree).

7. (Aug 09 #7) Let F be a field and K a finite-dimensional vector space over F. Let $n = \dim_F K$, and assume that $n > 1$.
   (a) Is it always true that $K \bigotimes_F K \cong M_n(F)$ as F-modules?
   (b) Now assume that K also has the structure of a commutative ring with 1, so being an F-vector space, K becomes an F-algebra. Recall that in this case $K \bigotimes_F K$ possesses a unique F-algebra structure such that $(a \otimes b) \cdot (c \otimes d) = ac \otimes bd$ for $a, b, c, d \in K$. Prove that $K \bigotimes_F K$ cannot be a field.
   Hint: Construct a non-trivial F-algebra homomorphism $K \bigotimes_F K \to K$.

8. (Aug 11 # 8) Let K be a field and let A, B be commutative K-algebras. We do not assume A or B is finite dimensional over K.
   (a) If the K-algebra $A \otimes_K B$ is a field, show that A and B must be fields, too. (Partial credit is given if you have to assume that A or B is finite dimensional over K.)
   (b) Provide an example of two field extensions A and B of degree 2 over K such that $A \otimes_K B$ is a field of degree 4 over K.
   (c) Compute $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ explicitly.

(d) Suppose K has characteristic $p > 0$ and that $A \mid K$ is a field extension such that there exists $\xi \in A$ such that $\xi \notin K$, but $\xi^p \in K$. Prove $A \otimes_K A$ is not a field.

9. (Aug 12 #5) Recall that if R is a commutative ring with 1 and A and B are R-algebras, then $A \otimes_R B$ also has the natural structure of an R-algebra.

   (a) Let K and L be fields of different characteristics. Prove that $K \otimes_{\mathbb{Z}} L = \{0\}$.

   (b) Let K and L be fields of the same positive characteristic p. Prove that $K \otimes_{\mathbb{Z}} L$ can be provided in a natural way with the structure of an $\mathbb{F}_p$-algebra, and that this $\mathbb{F}_p$-algebra is isomorphic to $K \otimes_{\mathbb{F}_p} L$. Deduce that $K \otimes_{\mathbb{Z}} L$ is nonzero.

   (c) Find an example of commutative rings A and B which are NOT fields such that $A \otimes_{\mathbb{Z}} B$ is a field. **Hint:** Use a suitable property of tensor products involving direct sums.

10. (Aug 13 #2) Let K and L be fields of characteristic 0. Prove that $K \bigotimes_{\mathbb{Z}} L$ is nonzero.

11. (Jan 14 #5)

    (a) Consider the abelian group
    $$A = \prod_{n \geq 2} \mathbb{Z}/n\mathbb{Z}.$$
    Show that this is not a torsion group by exhibiting an element of infinite order.

    (b) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} A \neq 0$. (Hint: this is $S^{-1}A$ for $S = \mathbb{Z} - \{0\}$.) Bonus: Determine $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} A)$.

12. (Aug 14 #2) Compute
    (a) $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$;
    (b) $\mathbb{Z}_{2014} \otimes_{\mathbb{Z}} \mathbb{Z}_{2013}$;
    (c) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_{2014}, \mathbb{Z}_{10})$ (Here $\mathbb{Z}_n$ is regarded as a $\mathbb{Z}$-module).

13. (Aug 14 #5) Let K be a field and $a \in K$. Consider K as a $K[x]$-module (denoted by K_a) via the homomorphism $\mathrm{ev}_a : K[x] \to K$ which is the identity on K and sends x to a. Let $K[[x]]$ be the power series ring, which is regarded as a $K[x]$-algebra in a natural way. Determine with proof the tensor product $K_a \otimes_{K[x]} K[[x]]$. (Hint: keep in mind if one needs to divide into cases depending on a.)

14. (Aug 15 #7) Let V be a finite dimensional vector space over a field F and let V^* be its dual. For $v \in V$ and $f \in V^*$, denote by $\phi_{v,f}$ the endomorphism of V defined by $\phi_{v,f}(w) = f(w)v$ for $w \in V$. Prove that there exists a well-defined F-linear map $\Phi : V \otimes_F V^* \to \mathrm{End}_F(V)$ satisfying $\Phi(v \otimes f) = \phi_{v,f}$ for all $v \in V$ and $f \in V^*$. Prove that Φ is an isomorphism.

15. (Jan 16 #8) Let K and L be finite extension fields of a field F of characteristic 0. Prove that $K \otimes_F L$ has no nonzero nilpotent elements.

16. (Aug 16 #5) Let V and W be vector spaces over a field F, and let $\{v_1, \ldots, v_\ell\}$ and $\{w_1, \ldots, w_\ell\}$ be elements of these vector spaces. Assume that the vectors $\{w_1, \ldots, w_\ell\}$ are linearly independent. Show that $\sum_{i=1}^{\ell} v_i \otimes w_i = 0$ implies that $v_1 = \cdots = v_\ell = 0$.

17. (Jan 17 #2) Consider a field K, and two finite extensions L, M of K. Consider the K-algebra $L \otimes_K M$ (with the usual multiplication $(a \otimes b)(c \otimes d) = ac \otimes bd$). Prove that $L \otimes_K M$ is a field if and only if any time an extension E/K contains subfields L' and M' which are K-isomorphic to L and M, the composite $L'M'$ has degree $[L'M' : K] = [L' : K][M' : K]$.

18. (Jan 17 #3) Let R be a commutative ring, and M, N be R-modules. Show that for any submodules $M' \subset M$ and $N' \subset N$, the induced map $M \otimes_R N \to (M/M') \otimes_R (N/N')$ has kernel given by $M' \otimes N + M \otimes N'$. Here $M' \otimes N$ and $M \otimes N'$ denote, respectively, the images of $M' \otimes_R N$ and $M \otimes_R N'$ in $M \otimes_R N$.

19. (Aug 17 #7) Consider the polynomial ring $R = F[x, y]$ in two variables over the field F and the ideal $I = (x, y)$ of R. Let $\phi : R \longrightarrow F$ be the F-algebra homomorphism with $\phi(x) = \phi(y) = 0$, which turns F into an R-module.
(a) Show that the R-modules $F \otimes_R F$ and F are isomorphic.
(b) Define maps $s, t : I \longrightarrow F$ by $s(f) = c_{1,0}$, respectively, $t(f) = c_{0,1}$ if $f = \sum_{i,j} c_{i,j} x^i y^j \in I$ (with $c_{i,j} \in F$ for all $i, j \in \mathbb{N}_0$). Verify that s and t are R-module homomorphisms.
(c) Prove that $x \otimes y - y \otimes x$ is not 0 in $I \otimes_R I$.
(d) Prove that I is not a flat R-module.

20. (Jan 18 #4) Let A be a finite abelian group of order n, p a prime divisor of n and $n = p^k m$ with $k, m \in \mathbb{N}$ such that $(p, m) = 1$. Denote by A_p the Sylow p-subgroup of A.
(a) Show that the abelian groups A_p and $\mathbb{Z}/p^k\mathbb{Z} \otimes_{\mathbb{Z}} A$ are isomorphic.
(b) Describe $\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} A$ as an abelian group without using tensor products but (certain) invariants of A.

Two more problems about tensor products:

21. Prove or disprove:
(a) $\mathbb{Q}(\sqrt{10}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{10})$ is isomorphic to $\mathbb{Q}(\sqrt{10})$ as a $\mathbb{Q}$-vector space.
(b) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to $\mathbb{Q}$ as a $\mathbb{Z}$-module.

22. Let I and J be ideals of a commutative ring R with 1. Show that $R/I \otimes_R R/J$ is isomorphic (as R-algebra) to $R/(I + J)$.

Chapter 5

Fields

5.1 General Field Theory

KNOW BASIC DEFINITIONS: Characteristic, prime field; field extension E/F (simple, algebraic, transcendental, finite, normal, separable, inseparable); degree $[E : F]$; $F(S), F[S]$ for subsets S of E/F. Minimum polynomial of an algebraic element $a \in E/F$; degree of a over F. Splitting field of a polynomial over F.

KNOW: Transitivity of degree $[K : F] = [K : E][E : F]$ if $K/E/F$;
$[K(\alpha) : K] = \deg(\mu_{\alpha|K})$ if α is algebraic over K with minimal polynomial $\mu_{\alpha|K}$.

KNOW HOW TO CONSTRUCT FIELD EXTENSIONS OF F: simple algebraic extension $E = F[x]/(p(x))$ for an irreducible polynomial $p(x)$ in $F[x]$: this is a simple algebraic extension of degree $[E : F] = \deg(p)$, generated by the image of x with minimal polynomial p. Simple transcendental extension: $E = F(x)$ = field of rational functions in x = field of fractions of $F[x]$.

KNOW ABOUT SPLITTING FIELDS: Existence and uniqueness of splitting fields; connection with normal extensions: a finite field extension L/K is normal iff L is the splitting field of some (non-constant) polynomial $f \in K[x]$; extension lemma for field isomorphisms.

KNOW ABOUT ALGEBRAICALLY CLOSED FIELDS: any field K has an algebraic extension $\overline{K}$ which is algebraically closed, called the *algebraic closure* of K; we have in particular $\overline{\mathbb{R}} = \mathbb{C}$ (FUNDAMENTAL THEOREM OF ALGEBRA).

KNOW ABOUT SEPARABLE POLYNOMIALS AND FIELD EXTENSIONS: definition of separability; the basic criterion: $f \in K[x]$ is separable iff $\gcd(f, D(f)) = 1$; consequence: fields of characteristic 0 and finite fields are *perfect*, i.e. all their algebraic extensions are automatically separable.

PRIMITIVE ELEMENT THEOREM: If L/K is finite and separable, then L is a simple extension of K, i.e. there exists $\alpha \in L$ such that $L = K(\alpha)$. (One can also show that L is a simple extension of K iff there are only finitely many intermediate fields between K and L.)

KNOW HOW TO: construct all finite fields $\mathbb{F}_q$ ($q = p^e$, split $x^{p^e} - x$ over $\mathbb{F}_p = \mathbb{Z}_p$).

AVOID THE FOLLOWING MISTAKES: If M/L and L/K are normal field extensions, M/K need **not** be normal; if $\mathrm{char}(K) = 0$, not all polynomials in $K[x]$ are separable (but the irreducible polynomials in $K[x]$ are); if $f \in K[x]$ for some field K satisfies $D(f) \neq 0$, this does **not** imply that f is separable (it does if f is irreducible); a polynomial in $K[x]$ which doesn't have any roots in K need **not** be irreducible (it is if $\deg(f) \leq 3$).

RELATED PROBLEMS

F is an arbitrary field.

1. (Apr 77 #2) If F is finite SHOW
   (a) $|F| = q$ is a power of a prime p,
   (b) F splits $x^q - x$ over $\mathbb{Z}_p$,
   (c) F^* is cyclic of order $q - 1$.

2. (Apr 77 #4b) If $p(x) \in F[x]$ is irreducible, SHOW there is a finite extension E/F containing a root of $p(x)$.

3. (Nov 77 #3) Give an example of an inseparable extension $E/\mathbb{Q}$ of degree 7.
   If you don't succeed, give an arbitrary example of an algebraic but inseparable field extension.

4. (Nov 77 #4) Define *finite* extension and *algebraic* extension; does either imply the other?

5. (May 78 #10) Give a polynomial whose splitting field is a field of 9 elements; repeat for 18 elements.

6. (Sep 82 #4) If E/F is algebraic and each $a \in E$ belongs to a normal sub-extension E_a ($F \subseteq E_a \subseteq E$), show E/F is normal.

7. (Sep 83 #3) (a) Show any finite subgroup of F^* (the multiplicative group of invertible elements of F) must be cyclic. (Done in class but you might recall the argument.)
   (b) Give an example of a finite nonabelian group contained in R^* for a ring R.

8. (Feb 84 #6) If $[F(a) : F]$ is odd show $F(a^2) = F(a)$.

9. (Sep 84 #7) Factor $x^8 - 1$ into irreducibles in $\mathbb{Z}_p[x]$ for *all* primes p.
   (Clarification: You should describe the prime factorization of $x^8 - 1$ in $\mathbb{Z}_p[x]$ for any given prime number p (distinguish cases!) but you needn't compute explicitly, as elements of $\mathbb{Z}_p$, those coefficients of the (monic) irreducible factors which are $\neq 0, \pm 1$.)

10. (1985 #3b) Show the set of all 2×2 matrices $\begin{pmatrix} a & b \\ \lambda b & a \end{pmatrix}$ over $\mathbb{F}_7$ form (under the usual matrix addition and multiplication) a ring of size 49. For which $\lambda \in \mathbb{F}_7$ is this a field?

11. (Sep 86 #1) If $F = \mathbb{F}_7$, show $p(x) = x^2 + 1$ and $p(x) = x^3 + x + 1$ are irreducible in $F[x]$, and show $F[x]/(p(x))$ are fields (give their cardinalities).

12. (Jan 87 #4) If $F \subseteq K \subseteq E$ with K/F finite, show that if K/F is separable (resp. normal, Galois), then also $K(a)/F(a)$ is separable (resp. normal, Galois) for any $a \in E$.

13. (May 89 #3) If a, b are algebraic over F of degrees m, n, show $[F(a,b) : F] \leq mn$, with equality if m, n are relatively prime. Give an example where the inequality is strict.

14. (Aug 89 #3) Show the set of all 2×2 matrices $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ over $\mathbb{F}_5$ form (under the usual matrix addition and multiplication) a field of size 25.

15. (Aug 89 #5) If $[E : F]$ is finite, show any ring endomorphism of E which fixes F is an automorphism of E.

16. (Aug 94 #6) Show that $F = \mathbb{F}_2[x]/(x^4 + x + 1)$ is a field of characteristic 2 containing a primitive 15-th root of unity. Exhibit such a root.

17. (Jan 95 #3) Let K and L be finite extensions of a field F, both contained in a field E. Let KL be the set of finite sums of products of members of K and L. Explain why KL is a subring of E that is finite-dimensional over F. From that, show that KL is a field and, in fact, the smallest subfield of E containing K and L.

18. (Aug 97 #3) Let $K(x)$ be the field of rational functions over the field K. Prove *Lüroth's Theorem*: for any nonconstant function $f \in K(x)$ the degree $[K(x) : K(f)]$ is finite. Can you describe $[K(x) : K(f)]$ in terms of f?

19. (Jan 98 #6) The finite field $\mathbb{F}_{32}$ of 32 elements can be constructed as the extension $\mathbb{F}_2(\beta)$ where β is a root of the polynomial $x^5 + x^2 + 1$ in $\mathbb{F}_2[x]$. Find the minimal polynomial of β^3 over $\mathbb{F}_2$.

20. (Aug 99 #5) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ($a_n \neq 0$) be a complex polynomial of degree $n > 1$, and f' its derivative. Let $\alpha_1, \ldots, \alpha_n$ be the n roots of f and $\alpha'_1, \ldots, \alpha'_{n-1}$ the $n-1$ roots of the derivative (listing each root as many times as its multiplicity). Show that the *average* of the roots of f equals the *average* of the roots of f'.
(Hint: Use the relations between the coeffiecients of a polynomial and the roots of that polynomial.)

21. (Aug 99 #8) If F is finite, show that every element $\alpha \in F$ is the sum $\alpha = \beta_1^2 + \beta_2^2$ of two squares (for some β_1, $\beta_2 \in F$).

22. (Aug 99 #9) If p is a prime number congruent to 1 mod 8, *show* that 2 is a "quadratic residue" mod p, i.e. there is an integer a such that $a^2 \equiv 2$ modulo p. (*Hint:* show there is an $\varepsilon \in \mathbb{Z}_p$ with $\varepsilon^4 = -1$, and consider $\alpha = \varepsilon + \varepsilon^{-1}$.)

23. (May 03, #8) Let $K = \mathbb{Z}/p\mathbb{Z}$ be the field of p elements (where p is a prime). For an integer $d > 0$, we let
$$\sigma_d = \sum_{x \in K} x^d.$$
Show that $\sigma_d = -1$ if $p - 1$ divides d and $\sigma_d = 0$ otherwise.

24. (Aug 05 #4) Let K be a $\mathbb{Q}$-subalgebra of $M_n(\mathbb{Q})$. If K is a field, prove that $[K : \mathbb{Q}] \leq n$.

25. (Jan 06 # 9) Prove that $\sqrt{2} + \sqrt[3]{3}$ is irrational.

26. (Jan 08 #7) Let F be a field.
(a) Show that if $a \in E$ is an element of a field extension of F with $[F(a) : F] = 7$, then $F(a^3) = F(a)$.
(b) Show that any subgroup of order 8 of the multiplicative group $F^\times$ of the field F *must* be cyclic. Is this also true of subgroups of order 16?

27. (Aug 08 #3) Prove or disprove the following statements about irreducibility.
(a) If $Gal(E|\mathbb{Q}) = S_n$ for E the splitting field over $\mathbb{Q}$ of a polynomial $f(x) \in \mathbb{Q}[x]$ of degree n, then $f(x)$ must be irreducible.
(b) If α is algebraic over $\mathbb{Q}$, then its minimum polynomial $\mu_{\alpha|\mathbb{Q}}(x)$ *must* be irreducible.
(c) If $A \in \mathbb{M}_{n\times n}(\mathbb{R})$, then its minimum polynomial $\mu_A(x)$ *must* be irreducible.

28. (Jan 12 # 8) Let F be a field of characteristic zero, let K and L be finite extensions of F and KL the compositum of K and L.
(a) Prove that $[KL : F] \leq [K : F][L : F]$.
(b) Assume that $[K : F]$ and $[L : F]$ are relatively prime. Prove that $[KL : F] = [K : F][L : F]$.
(c) Give an example where $K \cap L = F$ but $[KL : F] \neq [K : F][L : F]$.
(d) Assume that K/F and L/F are both Galois. Prove that $Gal(KL/F)$ is isomorphic to a subgroup of $Gal(K/F) \times Gal(L/F)$. (You need not prove that KL/F is Galois).
Note: The assertions of (a),(b) and (d) remain valid for F of positive characteristic, but part (a) has a shorter proof in the case of characteristic zero.

29. (Aug 12 #7) Let K/F be a field extension, let $\alpha, \beta \in K \setminus F$ be algebraic over F, and let $p = \deg_F(\alpha)$ and $q = \deg_F(\beta)$. Suppose that p and q are distinct primes and that $p > q$.
    (a) Prove that $[F(\alpha, \beta) : F] = pq$.
    (b) Prove that $\deg_F(\alpha\beta) = p$ or pq.
    (c) Give an example showing that it MAY happen that $\deg_F(\alpha\beta) = p$.

30. (Jan 13 #4) Let p be a prime, $\mathbb{F}_p$ a finite field of order p, and let F be a fixed algebraic closure of $\mathbb{F}_p$. For $n \in \mathbb{N}$, denote by $\mathbb{F}_{p^n}$ the unique subfield of order p^n inside F.
    (a) Prove that $\mathbb{F}_{p^n} \cup \mathbb{F}_{p^m}$ is a subfield if and only if m divides n or n divides m.

(b) For a subset S of $\mathbb{N}$, let

$$F(S) = \bigcup_{n \in S} \mathbb{F}_{p^n}.$$

Give an example (with proof) of an infinite set S for which $F(S)$ is a subfield and $F(S) \neq F$.

31. (Aug 13 #6) Let p be a prime and ζ a primitive p^{th} root of unity (in $\mathbb{C}$). Set $R := \mathbb{Z}[\zeta]$ and $K := \mathbb{Q}(\zeta)$.

(a) Show that R is a free $\mathbb{Z}$-module and $R \cap \mathbb{Q} = \mathbb{Z}$.

(b) Identify $Gal(K|\mathbb{Q})$ and show that the natural action of $Gal(K|\mathbb{Q})$ on K sends elements of R to itself (hence giving an action of $Gal(K|\mathbb{Q})$ on R).

(c) For any two integers m, n which are not divisible by p, show that the quotient $(1 - \zeta^m)/(1 - \zeta^n)$ is an element of R.
Hint: Reduce to the case where n divides m.

(d) Verify that $p = (1 - \zeta) \dots (1 - \zeta^{p-1})$.
Hint: manipulate the cyclotomic polynomial associated to ζ.

(e) Prove that $1 - \zeta$ is not a unit of R.

(f) Prove (using norms) that $1 - \zeta$ is an irreducible element of R. (It is true, but harder to prove, that $1 - \zeta$ is in fact a prime element of R.)

32. (Jan 14 #6) Let $K|F$ be an extension of finite fields, and let L, M be subfields of K containing F. Assume that $L \cap M = F$.

(a) Show that the degrees $[L : F]$ and $[M : F]$ are relatively prime.
Hint: How many subfields of a given order does a finite field have?

(b) Now assume additionally that $L = F(\alpha)$, $M = F(\beta)$ and $K = F(\alpha, \beta)$ for some $\alpha, \beta \in K$. Prove that $K = F(\alpha + \beta)$.

5.2 Galois Theory

In this section, L/K always denotes a *finite* field extension.

KNOW THE BASIC DEFINITIONS AND FACTS: The *Galois group* of L/K is $G(L|K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(a) = a \quad \text{for all} \quad a \in K\}$; recall that we always have $|G(L|K)| \leq [L : K]$; for any subgroup H of $\mathrm{Aut}(L)$, the *fixed field* of H is $\mathrm{Fix}(H) := \{\alpha \in L \mid \sigma(\alpha) = \alpha \quad \text{for all} \quad \sigma \in H\}$. L/K is *Galois'* iff it is normal and separable iff L is the splitting field over K of a separable polynomial $f \in K[x]$ iff $|G(L|K)| = [L : K]$ iff $\mathrm{Fix}(G(L|K)) = K$.

KNOW ARTIN'S THEOREM: $[L : \mathrm{Fix}(H)] = |H|$ for any finite subgroup H of $\mathrm{Aut}(L)$.
Consequence: If L/K is any finite field extension, then $|G(L|K)|$ divides $[L : K]$.

KNOW THE FUNDAMENTAL THEOREM OF GALOIS THEORY: If L/K is Galois, the maps $M \mapsto G(L|M)$ and $H \mapsto \mathrm{Fix}(H)$ are inverse (and inclusion reversing) bijections between $\{M \mid M$ is an

intermediate field, L/M/K } and $\{H \mid H \text{ is a subgroup of } G(L|K)\}$. Explicitly:
$\text{Fix}(G(L|M)) = M$ and $G(L|\text{Fix}(H)) = H$;
keep in mind that an intermediate field M corresponds to a subgroup H of *index* $[M : K]$ in $G(L|K)$, and that $|H| = |G(L|K)| \div [M : K] = [L : M]$.

KNOW THE CORRESPONDENCE BETWEEN NORMAL SUBEXTENSIONS AND NORMAL SUBGROUPS: M/K is normal iff $\sigma(M) = M$ for all $\sigma \in G(L|K)$ iff $G(L|M)$ is a normal subgroup of $G(L|K)$; if this is the case, then any element of $G(M|K)$ can be extended to an element of $G(L|K)$, and $G(M|K) \cong G(L|K)/G(L|M)$.

Consequence: If L/K is Galois' and $\alpha \in L$, then $G(L|K)$ permutes the roots of the minimal polynomial $\mu_{\alpha|K}$ *transitively* (choose M to be the splitting field over K of $\mu_{\alpha|K}$).

KNOW THAT EXTENSIONS OF FINITE FIELDS ARE CYCLIC: An extension L/K of finite fields is always Galois'; if $K = \mathbb{F}_q$ and $[L : K] = n$, then $G(L|K)$ is the cyclic group of order n generated by the *Frobenius automorphism* σ with $\sigma(\alpha) = \alpha^q$ for all $\alpha \in L$.

KNOW THE BASIC FACTS ABOUT ROOTS OF UNITY: $x^n - 1$ is separable over K iff $\text{char}(K)$ does not divide n (hence always if $\text{char}(K) = 0$); denote by K_n its splitting field over K. Then the roots of $x^n - 1$ form a cyclic subgroup U_n of order n of K_n^*; any generator ζ_n of U_n is called a *primitive* n^{th} root of unity, and we have $K_n = K(\zeta_n)$. K_n/K is Galois' with $G(K_n|K)$ isomorphic to a subgroup of $\mathbb{Z}_n^*$. In particular, $G(K_n|K)$ is ALWAYS ABELIAN but NOT necessarily cyclic. If $K = \mathbb{Q}$, the irreducibility of the cyclotomic polynomials implies $G(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong \mathbb{Z}_n^*$. Hence for $n = p^m$ with an odd prime p and $m \in \mathbb{N}$, $G(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ is cyclic ($\cong \mathbb{Z}_{(p-1)p^{m-1}}$); note that this is not true for $p = 2$. $\mathbb{Q}(\zeta_n)$ is usually called a *cyclotomic field*.

RELATED PROBLEMS

1. (May 78 #11) Describe all intermediate fields of E/F if E/F is Galois with group $Gal(E/F) = S_3$.
2. (May 80 #6) If $F = \mathbb{Q}(\beta)$ for a primitive n-th root of unity β, and $b^n = a \in F$ where $a \notin F^n$ is not an n-th power in F, show $G(F(b)/F)$ is abelian.
3. (Mar 83 #7) (a) SHOW $E = \mathbb{F}_{p^6}$ is Galois over $F = \mathbb{F}_p$.
   (b) Express the trace $Tr_{E/F}(x)$ as a polynomial in x, and show there is an x with $Tr_{E/F}(x) \neq 0$.
   (c) Show $B(x, y) := Tr_{E/F}(xy)$ is a nondegenerate bilinear form on $E \times E$ to F.
4. (Sep 83 #8) If $E/\mathbb{Q}$ is Galois and $B(x, y) := Tr_{E/\mathbb{Q}}(xy)$ (you may assume this is a nondegenerate bilinear form on $E \times E$ to $\mathbb{Q}$), find the adjoints σ^* of the elements σ of the Galois group $G(E/\mathbb{Q})$ with respect to the bilinear form B.
5. (1985 #4) Let E_n be the splitting field of $x^n - 1$ over $\mathbb{Q}$.
   (a) What is $[E_n : \mathbb{Q}]$?
   (b) What is $|G_n|$ for $G_n = Gal(E_n/\mathbb{Q})$? PROVE G_n is abelian.
   (c) SHOW G_{16} is not cyclic.

6. (Fall 87 #8) If $E/\mathbb{Q}$ is a splitting field of an irreducible polynomial f of degree 8, and $a \in E$ is a root of f so that f splits over $\mathbb{Q}(a)$ into 2 linear and 3 quadratic factors, find the possible orders of $Gal(E/\mathbb{Q})$ and show that this group is always solvable.

7. (May 89 #6) If E/F is Galois with $Gal(E/F)$ simple, for any element $a \in E$ which is not in F show that E is a splitting field for the minimum polynomial of a over F.

8. (May 90 #3) If $E/\mathbb{Q}$ is a finite Galois extension inside $\mathbb{C}$ with $Gal(E/\mathbb{Q})$ simple of order > 2, show the imaginary unit i CANNOT belong to E.

9. (Jan 92 #3) If ω is a primitive cube root of 1, determine whether $\mathbb{Q}(\omega\sqrt[3]{2})$ is a Galois extension of $\mathbb{Q}$. Give reasons.

10. (Aug 94 #7) Let ζ_n be a primitive n-th root of unity in $\mathbb{C}$ for $n > 2$. Show that the fixed field of $\mathbb{Q}(\zeta_n)$ under complex conjugation is $\mathbb{Q}(\zeta_n + \bar{\zeta}_n) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. (*Hint:* write $\bar{\zeta}_n$ as a power of ζ_n and find a polynomial of low degree satisfied by ζ_n over $\mathbb{Q}(\zeta_n + \bar{\zeta}_n)$.)

11. (Jan 95 #8) Give an example of a polynomial $f(x) \in \mathbb{Q}[x]$ having all these properties: (1) degree 4; (2) no rational roots; (3) no repeated factors in $\mathbb{Q}[x]$; (4) its Galois group over $\mathbb{Q}$ is cyclic of order 2.

12. (Aug 95 #6) Let $E/\mathbb{Q}$ be a splitting field of $x^3 - 9x + 12$. Show that there is a single normal extension $F/\mathbb{Q}$ with $E \supsetneq F \supsetneq \mathbb{Q}$. Find $[F : \mathbb{Q}]$.

13. (Aug 96 #6) Let E/F be a finite Galois extension with Galois group G. The *Normal Basis Theorem* states that there is an element u in E whose images under the elements of G form an F-basis of E. Prove that for any subgroup H of G, the subfield corresponding to H in the Galois correspondence is $F(u_H)$ for $u_H = \sum_{h \in H} h(u)$.

14. (Aug 97 #1ac) Let p be a prime number and F a field containing p distinct p-th roots of unity. Let E/F be a Galois extension for which $[E : F] = p$.
    (a) Prove that the Galois group $Gal(E/F)$ is cyclic of order p.
    (b) Prove that there is an element $b \in E \backslash F$ with $b^p \in F$.

15. (Aug 98 #7) Suppose that K is a finite Galois extension of the rational field $\mathbb{Q}$ which contains $\sqrt{3}$ and has cyclic Galois group $Gal(K/\mathbb{Q})$. Show that $L = \mathbb{Q}(\sqrt{3})$ is the only quadratic extension of $\mathbb{Q}$ contained in K.

16. Let E be a separable extension of the field F, with $[E : F] = n$. Use Galois theory to find an upper bound $B(n)$ for the number of intermediate fields K, $F \subseteq K \subseteq E$, that depends only on n. You don't need to make the bound $B(n)$ very tight!

17. (Aug 02 #9) Construct a Galois extension of $\mathbb{Q}$ of degree 3.

18. (Jan 04 #5) Let ζ be a primitive 9-th root of unity. Let $K = \mathbb{Q}(\zeta)$ and $F = \mathbb{Q}(\zeta + \zeta^{-1})$.
    (a) Show that $[K : F] = 2$.
    (b) Show that the extension $F \mid \mathbb{Q}$ is normal.

19. (Aug 04 #4) Let L/K be a finite Galois extension. Suppose there exists an element $\alpha \in L$ and another root α' of the minimal polynomial $\mu_{\alpha|K}$ of α over K such that the difference $\alpha' - \alpha$ is an element of $K \setminus \{0\}$.
(a) Prove that the characteristic p of K is different from 0 and that p divides $[L : K]$.
(b) Give an example of an extension L/K and elements α, α' as described above.

20. (Jan 06 #10) Find all subfields of the field $Q(\zeta_3, \sqrt[3]{2})$ for $\zeta_3 \in \mathbb{C}$ a primitive cube root of unity.

21. (Aug 06 #8) Let $M \mid K$ be a Galois extension of degree 270. Show that there is an intermediate extension $M \mid L \mid K$ with $[L : K] = 30$.

22. (Aug 09 #6) Let K/F be a finite extension of fields, and let $\alpha, \beta \in K$ be such that $K = F(\alpha, \beta)$. Let $n = [F(\alpha) : F]$ and $m = [F(\beta) : F]$, and assume that n and m are relatively prime.
(a) Prove that $[K : F] = nm$.
(b) Assume that K/F is Galois. Let $\mu_{\alpha,F}(x)$ and $\mu_{\beta,F}(x)$ be the minimal polynomials of α and β over F, respectively. Let $\alpha' \in K$ be a root of $\mu_{\alpha,F}(x)$, and let β' be a root of $\mu_{\beta,F}(x)$. Prove that there exists a unique $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\alpha) = \alpha'$ and $\sigma(\beta) = \beta'$.
(c) Again assume that K/F is Galois. Let S be the set of all elements $c \in F$ such that $F(\alpha + c\beta) \neq K$. Prove that $|S| \leq nm$.

23. (Aug 10 #6) Let $K = \mathbb{Q}(\sqrt[3]{3}, \sqrt[5]{5})$, the field obtained from $\mathbb{Q}$ by adjoining $\sqrt[3]{3}$ and $\sqrt[5]{5}$.
(a) Prove that $[K : \mathbb{Q}] = 15$.
(b) Let $L \subseteq \mathbb{C}$ be the Galois closure of K over $\mathbb{Q}$, that is, L is the minimal Galois extension of $\mathbb{Q}$ which contains K. Describe L explicitly in the form $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$, determine $[L : \mathbb{Q}]$ and describe the elements of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ by their actions on $\alpha_1, \ldots, \alpha_t$.
(c) Prove that $K = \mathbb{Q}(\sqrt[3]{3} + \sqrt[5]{5})$.

24. (Aug 11 #4b) Let K/F be a finite extension of finite fields. Show the norm map $N_{K/F} : K \to F$ is surjective.

25. (Aug 12 #8) In this problem you may use the following fact without proof: for any finite group G there exists a Galois extension M/L with $Gal(M/L) \cong G$.

    (a) Prove that there exists a field extension K/F such that $[K : F] = 4$ and there are no intermediate fields between F and K other than F and K. **Hint:** First reduce the question to a purely group-theoretic problem. Partial credit will be given for such reduction.

    (b) Is it possible to construct an extension satisfying (a) if F is finite? Justify your answer.

    (c) Is it possible to construct an extension satisfying (a) if K is contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$ for some n (where ζ_n is a primitive n^{th} root of unity)? Justify your answer.

26. (Jan 13 #5) Let $\omega = e^{2\pi i/3}$ and consider the field $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

    (a) Prove that $[K : \mathbb{Q}] = 6$.

    (b) Prove that $K/\mathbb{Q}$ is a Galois extension.

(c) Let M/L be any finite Galois extension. Prove that an element $\gamma \in M$ is primitive for M/L (that is, $L(\gamma) = M$) if and only if $\sigma(\gamma) \neq \gamma$ for any $\sigma \in \mathrm{Gal}(M/L) \setminus \{1\}$.

(d) Now prove that $\gamma = \sqrt[3]{2} + \omega$ is a primitive element for $K/\mathbb{Q}$.

(e) Let $x^6 + a_5x^5 + \ldots + a_0$ be the minimal polynomial of γ over $\mathbb{Q}$. Prove that $a_5 = 3$ without actually computing the minimal polynomial.

27. (Jan 16 #6) Let $K = \overline{\mathbb{Q}}$ be the algebraic closure of the rationals in $\mathbb{C}$, i.e., the set of elements in the complex numbers which are algebraic over the rationals. By Zorn's lemma, there exists a maximal subfield of K, say E, which does not contain the square root of 2. Prove that every finite normal extension of E has cyclic Galois group. (Hint: reduce this to a question about groups.)

28. (Jan 16 #7) Let ϵ be a primitive 16th root of unity in the complex numbers. Set $s = \sqrt{2} \cdot \epsilon$. Let $E = \mathbb{Q}[\epsilon]$, where $\mathbb{Q}$ is the field of rational numbers, and set $f(X) = X^8 + 16 \in \mathbb{Q}[X]$. Show that s is a root of $f(X)$. Prove that $\sqrt{2} \in \mathbb{Q}[\epsilon]$, and hence that $f(X)$ splits completely over E. If $G = Gal(E/\mathbb{Q})$, prove that no nonidentity element of G fixes s. Prove that $f(X)$ is irreducible over $\mathbb{Q}$.

29. (Aug 17 #6) Let $M|K, M|L, K|F, L|F$ be finite field extensions. Assume that for $\alpha, \beta \in M$, $K = F(\alpha)$, $L = F(\beta)$ and $M = F(\alpha, \beta)$. Set $a = [K : F]$ and $b = [L : F]$.
(a) If $K|F$ and $L|F$ are Galois, show that also $M|F$ is Galois.
(b) If $K|F$ and $L|F$ are Galois, prove that $[M : F]$ divides ab.
(c) Give an example of M, K, L, F as above (but without the Galois assumption) such that $[M : F]$ does *not* divide ab.

30. (Jan 18 #8) Let $M \mid K \mid F$ be a tower of finite field extensions such that $M \mid F$ and $K \mid F$ are both Galois. Assume that the Galois group $G(M|K)$ is cyclic. Prove that $L \mid F$ is Galois for every intermediate field L with $M \mid L \mid K$.

5.3 Finding Galois Groups

Here are a few remarks (certainly no complete list!) which might help in finding Galois groups in a concretely given situation. Let us first introduce some notation. If a *separable* polynomial $f \in K[x]$ of degree $n > 0$ is given and L is the (up to K-isomorphism uniquely determined) splitting field of f over K, we set $G(f|K) := G(L|K)$ and call this the *Galois group of* f over K.

(1) If $R_f := \{\alpha_1, \ldots, \alpha_n\}$ is the set of roots of f in L, the restriction of elements of $G(f|K)$ to R_f defines an *injective* group homomorphism *res* from $G(f|K)$ into the group of all permutations of R_f. Hence $G(f|K)$ can be identified with a subgroup of S_n.

(2) $G(f|K)$ induces a *transitive* action on R_f if and only if f is irreducible. So for an irreducible polynomial f of degree 3 or 4, there are only the following options:
$n = 3$: $G(f|K) = S_3$ or A_3
$n = 4$: $G(f|K) = S_4$ or A_4 or a Sylow 2-subgroup of S_4 (hence $\cong D_8$) or a subgroup generated by a 4-cycle or the unique normal subgroup V ($\cong \mathbb{Z}_2 \times \mathbb{Z}_2$) of S_4 with $|V| = 4$.

(3) If $K = \mathbb{Q}$, $n = 3$, f is irreducible and *not* all roots of f are real, then $G(f|K) = S_3$. (Why?)

(4) Recall that $G(x^n - 1|\mathbb{Q}) = \mathbb{Z}_n^*$. This provides you (together with the subfields of $\mathbb{Q}(\zeta_n)$) with a couple of nice *abelian* Galois groups. (In fact, by a famous theorem due to Kronecker and Weber, *any* finite Galois extension M of $\mathbb{Q}$ with abelian $G(M|\mathbb{Q})$ is a subfield of a cyclotomic field.)

(5) An important number associated with the polynomial f (which we assume to be monic here) is its *discriminant* $D_f := \prod_{i<j}(\alpha_i - \alpha_j)^2$, where again $R_f = \{\alpha_1, \ldots, \alpha_n\}$. D_f has the following properties (see also Problem (24) below):
(i) $D_f \in K$ (since it is invariant under $G(f|K)$)
(ii) $D_f \neq 0$ (since we assumed that f is separable)
(iii) $\sqrt{D_f} = \prod_{i<j}(\alpha_i - \alpha_j)$ is an element of the splitting field L of f
(iv) If $\mathrm{char}(K) \neq 2$, an element $\sigma \in G(f|K)$ fixes $\sqrt{D_f}$ iff σ is in A_n. Hence $G(f|K) \leq A_n$ iff $\sqrt{D_f} \in K$.
(v) D_f is a polynomial expression in the coefficients of f. We have the following formulas:
$f(x) = x^2 + ax + b \Rightarrow D_f = a^2 - 4b$
$f(x) = x^3 + ax^2 + bx + c \Rightarrow D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$, in particular
$f(x) = x^3 + px + q$ (standard form) $\Rightarrow D_f = -4p^3 - 27q^2$
$f(x) = x^4 + px^2 + qx + r \Rightarrow D_f = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$
$f(x) = x^4 + ax^3 + b \Rightarrow D_f = -27a^4b^2 + 256b^3$

Related Problems

In Problems 1 - 14 below, a field F is given together with a polynomial $f(x) \in F[x]$, respectively an element β which is algebraic over F. Determine the Galois group $G = G(f|F)$, respectively $G = G(F(\beta)|F)$ (also decide whether $F(\beta)/F$ is Galois), and answer the questions in brackets.

1. (Apr 77 #6) $F = \mathbb{Q}$, $f = x^3 + 5$ (show f is irreducible but G is not of order 3; is $G(f|\mathbb{Q})$ solvable?)
2. (Jan 81 #2) $F = \mathbb{Q}$, $\beta =$ primitive 7-th root of unity (find the minimum polynomial of β, find $[\mathbb{Q}(\beta) : \mathbb{Q}]$, find all subfields).
3. (Jan 82 #2) $F = \mathbb{Q}$, $f = x^3 + 5x - 5$ (show f is irreducible, find its real roots; is $G(f|\mathbb{Q})$ solvable?)
4. (Sep 82 #5) $F = \mathbb{Q}$, $f = x^4 + 2x^2 + 2$.
5. (March 83 #2) $F = \mathbb{Q}$, $\beta = (1 + \sqrt{2})/(1 + \sqrt{3})$.
6. (Sep 86 #4) $F = \mathbb{Q}$, $f = x^4 + 1$.
7. (Aug 88 #5; Sep 80 #7) $F = \mathbb{Q}$, $f = x^4 - x^2 - 6$.
8. (Jan 87 #3) $F = \mathbb{Q}$, $f = x^4 - x^2 - 2$.

9. (May 91 #5) $F = \mathbb{Q},\ f = x^4 - 2$ (find G, identify all subfields of degree 4 over Q with their corresponding subgroups).

10. (Jan 94 #2) $F = \mathbb{Q},\ f = x^4 - 2$ (show G isomorphic to the dihedral group of order 8).

11. (Jan 95 #7) $F = \mathbb{Q},\ f = x^4 - 2x^2 - 2$ (show f irreducible, describe G as permutations of roots).

12. (Aug 95 #3) $F = \mathbb{Q},\ f = x^4 - 4$ (describe G as automorphisms, find all subfields).

13. (Jan 97 #5) $F = \mathbb{Q},\ f = x^4 - 5$ (describe G as a group of permutations of the roots).

14. (Jan 98 #5a) $F = \mathbb{Q},\ f = x^5 + 5x^3 - 20x + 10$.

15. (Nov 77 #8) Find $Gal(E/\mathbb{Q})$ if $E = \mathbb{Q}(i, \beta)$ for β a primitive n-th root of unity for odd $n > 1$.

16. (Sep 78 #4) (a) If f is irreducible of degree 5 over $\mathbb{Q}$, show $G(f/\mathbb{Q})$ contains an element of order 5.
    (b) Show $G(x^4 + 1/\mathbb{Q})$ has NO element of order 4.
    (c) Show $G(x^4 + x^3 + 1/\mathbb{Q})$ HAS an element of order 4.

17. (Jan 79 #6; Sep 79 #6) Find $Gal(E/\mathbb{Q})$ for $E = \mathbb{Q}(\sqrt{2}, i)$ or $E = \mathbb{Q}(i + \sqrt{2})$.

18. (Sep 83 #4) If $x^4 + ax^2 + 1$ is separable and irreducible over F, find all roots and their relationships, find G. Show that F must be infinite.

19. (Sep 84 #3) If $E/\mathbb{Q}$ is Galois of degree 4, prove $E = \mathbb{Q}(\beta)$ for a root β of a polynomial $x^4 + ax^2 + b \in \mathbb{Q}[x]$; show $Gal(E/\mathbb{Q})$ is cyclic iff b is NOT in $\mathbb{Q}^2$.

20. (Jan 89 #4; Feb 84 #2) (a) Find $Gal(x^3 - 2/\mathbb{Q})$.
    (b) Find $f(x) \in \mathbb{Q}[x]$ with $Gal(f/\mathbb{Q}) = \mathbb{Z}_2 \times S_3$.

21. (Aug 89 #8) If $\beta = \sqrt{2 + \sqrt{2}}$, show $\mathbb{Q}(\beta)/\mathbb{Q}$ is Galois with G cyclic; set up the Galois correspondence.

22. (Sep 93 #6) $F = \mathbb{Q},\ f = x^5 - 6x + 3$. Prove f is
    (a) irreducible,
    (b) has exactly 3 real roots,
    (c) $G(E/L)$ contains a transposition of roots of f for any real subfield L of the splitting field E of f over $\mathbb{Q}$,
    (d) $G(E/Q) = S_5$,
    (e) $0 < r \in \mathbb{Q}, \sqrt{r} \notin \mathbb{Q} \Longrightarrow \sqrt{r} \notin E$.

23. (Jan 98 #5) The Galois group G of F of a polynomial $f(x) \in F[x]$ of degree 4 is known to contain a subgroup isomorphic to the dihedral group D_8.
    (a) Show that $f(x)$ is irreducible.
    (b) If some root r_i of $f(x)$ lies in the subfield $F(r_j, r_k)$ generated by two other roots, show $F(r_j, r_k)$ is a splitting field for $f(x)$ and that $G = D_8$.

24. (Jan 00 #7) Suppose that f is an irreducible polynomial of degree n with rational coefficients. Let K be a splitting field for f over the rationals $\mathbb{Q}$, and let $r_1, \ldots, r_n$ be the roots of f in K, with $a = \prod_{i<j}(r_i - r_j)$.
(a) *Show* that the roots of f are distinct.
(b) If the product a is not rational, *show* the Galois group $Gal(K/\mathbb{Q})$ contains an element which yields an odd permutation of the roots.
(c) If the product a is not rational, *show* that K contains at least one quadratic subfield.

25. (Jan 00 #8) Let ζ be primitive 3rd root of unity, $K = \mathbb{Q}(\zeta)$, and $L = K(\sqrt[3]{2})$.
(a) *Show* that L/K is a Galois extension, and *determine* its Galois group $G := Gal(L/K)$.
(b) Considering L as vector space over K, *determine* all K-linear functionals $f : L \to K$ which are *G-invariant* (i.e. $f(\sigma(a)) = f(a)$ for all $\sigma \in G$ and all $a \in L$).

26. (Aug 01 #8) Find the Galois group of $f(x) = x^{13} - 1$ over the rationals $\mathbb{Q}$ (i.e. $Gal(K/\mathbb{Q})$ for K the splitting field of $f(x)$ over $\mathbb{Q}$).

27. (Aug 03 #5) Choose your favorite one, denoted by G, between the Klein four group (i.e. $\mathbb{Z}_2 \times \mathbb{Z}_2$) and the dihedral group D_8 of order 8. Provide an example of an irreducible degree 4 polynomial whose Galois group over $\mathbb{Q}$ is isomorphic to G. Show your work.

28. (Jan 05 #6) Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4, α a root of f, $K := \mathbb{Q}(\alpha)$ and L the splitting field of f over $\mathbb{Q}$. Assume that $[L : \mathbb{Q}] \neq 4$.
(a) Show that $G(L|\mathbb{Q})$ is isomorphic to S_4, A_4 or D_8.
(b) Show that $G(L|\mathbb{Q})$ is isomorphic to D_8 if K contains a subfield F such that $[F : \mathbb{Q}] = 2$.
(You might use the subgroup structure of S_4 for free.)

29. (Aug 05 #5) Let K be a field, $f \in K[x]$ a *reducible* separable polynomial of degree 4, L the splitting field of f over K and $G = G(L|K)$ the corresponding Galois group. List *all* (but no more!) possibilities for G in the following two cases:
(a) $K = \mathbb{Q}$
(b) $K = \mathbb{F}_p$, where p is a prime number

30. (Jan 08 #8) (a) Find a splitting field E of the polynomial $x^4 + 3x^3 + 4x^2 + 3x + 3$ over the rationals $F = \mathbb{Q}$, and find its degree $[E : F]$.
(Hint: First factorize over $\mathbb{Q}$, and then write $E = F(\alpha, \beta)$ for an easy pure imaginary α and a real β.)
(b) Find the Galois group $Gal(E/F)$ of the extension field (describe all the automorphisms by their actions on α, β).
(c) Diagram the lattice of subgroups of the Galois group and the corresponding lattice of sub-field-extensions of E/F.

31. (Aug 08 #8) This problem involves finding a seventh degree polynomial whose Galois group is isomorphic to S_7.
(a) Prove that if p is prime then any transposition τ and p-cycle σ together generate all of S_p.
(b) Prove that if p is a prime number, and E a splitting field over $\mathbb{Q}$ for an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree p with exactly $p - 2$ real roots, then the Galois group $Gal(E|\mathbb{Q}) = S_p$.

(c) Give a counter-example to the statement in part (b) if the degree of the polynomial is not prime.
(d) *Exhibit* (with proof) an irreducible polynomial of degree 7 over the rationals whose Galois group is S_7.

32. (Jan 09 #7) Let $p(x) = x^4 - 2 \in \mathbb{Q}[x]$.
(a) Find a splitting field K for $p(x)$. Describe K in the form $\mathbb{Q}(\alpha, \beta)$ for some $\alpha, \beta \in \mathbb{C}$.
(b) Determine the Galois group $Gal(K|\mathbb{Q})$ and describe its elements by their actions on α and β.
(c) Which (well-known) group is $Gal(K|\mathbb{Q})$ isomorphic to? Prove your answer.

33. (Aug 11 #6) (a) Suppose that, for some prime number p, $G = C_p \times \ldots \times C_p$ is a direct product of n copies of the cyclic group C_p of order p. How many subgroups does G have of order p? How many does it have of order p^{n-1}? Explain.
(b) Now let $p_1, \ldots, p_r$ be distinct prime numbers. Show that $F := \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_r}]$ is an abelian Galois extension of $\mathbb{Q}$.
(c) Suppose that $a = p_{i_1} \ldots p_{i_m}$ (with distinct factors) is a nontrivial product of some of the primes $p_1, \ldots, p_r$. Let $b \neq a$ be another such element. Show that $\mathbb{Q}[\sqrt{a}] \neq \mathbb{Q}[\sqrt{b}]$. Now use (a) to determine precisely the Galois group of $F/\mathbb{Q}$. Carefully justify your answer.
(d) Show that the numbers $\sqrt{p_1}, \ldots, \sqrt{p_r}$ are linearly independent over $\mathbb{Q}$, and that $\sqrt{p_1} + \ldots + \sqrt{p_r}$ is a primitive element of $F/\mathbb{Q}$.

34. (Aug 13 #5) Let F be a field and $f(x) = x^4 + 1 \in F[x]$.

    (a) Determine for which characteristic of F $f(x)$ is separable.

    (b) Assume that $f(x)$ is separable and irreducible over F, and denote by K the splitting field of $f(x)$ over F. Determine the Galois group $Gal(K|F)$.

    (c) If $f(x)$ is irreducible over F, prove first that F is infinite, and then that the characteristic of F is 0.

35. (Jan 14 #7) Consider the real number $u = \sqrt{3 + \sqrt{11}}$.

    (a) Determine the minimal polynomial for u over $\mathbb{Q}$, and justify that it is the minimal polynomial.

    (b) Is $\mathbb{Q}[u]$ the splitting field for the minimal polynomial of u? (Hint: consider which roots are real and which are complex.)

    (c) Determine the Galois group of the splitting field. (Hint: What is the degree of the field extension?)

36. (Aug 14 #7) Let $f(x) = x^5 - 2 \in \mathbb{Z}[x]$.
(a) Determine the splitting field F of $f(x)$ over $\mathbb{Q}$;
(b) Determine the Galois group of $f(x)$ over $\mathbb{Q}$;
(c) List all the subfields K of F such that $[K : \mathbb{Q}] = 4$.

37. (Aug 15 #8) Consider the polynomial $x^6 - 3$ over the rational numbers. What is the degree of its splitting field, and what is the splitting field? Describe the Galois group of the splitting field as a subgroup of the symmetric group S_6. Is it abelian?

38. (Aug 16 #3) Let $f(x) = x^4 - x^2 + 1$.

    (a) Describe a splitting field E for f over $\mathbb{Q}$ (in particular, find its degree).

    (b) Describe the Galois group of E and all of its subfields.

39. (Jan 17 #1) Consider the polynomial $f(X) = X^4 - 2X^2 - 6$. Prove this polynomial is irreducible. Describe the splitting field of this polynomial (including its degree over $\mathbb{Q}$), and the Galois group of this splitting field (hint: pay attention to which roots are real and which are complex).

40. (Jan 18 #7) (a) Construct, using cyclotomic fields, a Galois extension K of $\mathbb{Q}$ of degree 3. Include arguments.
    (b) Find, explicitly, a polynomial $f(x) \in \mathbb{Q}[x]$ such that your field K in (a) is the splitting field of $f(x)$ over $\mathbb{Q}$.