

ALGEBRA QUALIFYING EXAM PROBLEMS

Kent State University
Department of Mathematical Sciences

Compiled and Maintained
by
Donald L. White

Version: May 27, 2009

CONTENTS

LINEAR ALGEBRA AND MODULES

General Matrix Theory	1
Canonical Forms, Diagonalization, and Characteristic and Minimal Polynomials	1
Linear Transformations	4
Vector Spaces	5
Inner Product Spaces	6
Modules	6

GROUP THEORY

General Group Theory	8
Cyclic Groups	10
Homomorphisms	11
Automorphism Groups	11
Abelian Groups	12
Symmetric Groups	13
Infinite Groups	14
p -Groups	15
Group Actions	16
Sylow Theorems	18
Solvable and Nilpotent Groups, Commutator and Frattini Subgroups	22

RING THEORY

General Ring Theory	25
Prime, Maximal, and Primary Ideals	28
Commutative Rings	29
Domains	31
Polynomial Rings	32
Non-commutative Rings	33
Local Rings, Localization, Rings of Fractions	34
Chains and Chain Conditions	35

FIELD THEORY

General Field Theory	36
Algebraic Extensions	38
Normality and Splitting Fields	39
Separability	40
Galois Theory	42
Cyclotomic Extensions	45
Finite Fields	45
Cyclic Extensions	47
Radical Extensions and Solvability by Radicals	47
Transcendental Extensions	47

LINEAR ALGEBRA

General Matrix Theory

1. Let $m > n$ be positive integers. Show that there do not exist matrices $A \in \mathbb{R}^{m \times n}$ and $B \in \mathbb{R}^{n \times m}$ such that $AB = I_m$, where I_m is the $m \times m$ identity matrix.
2. Let A and B be nonsingular $n \times n$ matrices over \mathbb{C} .
 - (a) Show that if $A^{-1}B^{-1}AB = cI$, $c \in \mathbb{C}$, then $c^n = 1$.
 - (b) Show that if $AB - BA = cI$, $c \in \mathbb{C}$, then $c = 0$.
3. Let A be a strictly upper triangular $n \times n$ matrix with real entries, and let I be the $n \times n$ identity matrix. Show that $I - A$ is invertible and express the inverse of $I - A$ as a function of A .
4.
 - (a) Give an example of a complex 2×2 matrix which does not have a square root.
 - (b) Show that every complex non-singular $n \times n$ matrix has a square root. [Hint: Show first that a Jordan block with non-zero eigenvalue has a square root.]

5. Let $T : \mathbb{R}^3 \rightarrow \mathbb{R}^4$ be given by $T(v) = Av$, where $A = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 0 & 3 \\ 0 & 1 & 0 \\ 3 & 4 & 2 \end{bmatrix}$.

- (a) Find the dimension of the null space of T .
- (b) Find a basis for the range space of T .

Canonical Forms, Diagonalization, and Characteristic and Minimal Polynomials

6. State and prove the Cayley-Hamilton Theorem.
7. Show that if A is an $n \times n$ matrix, then A^n can be written as a linear combination of the matrices $I, A, A^2, \dots, A^{n-1}$ (that is, $A^n = \alpha_0 I + \alpha_1 A + \alpha_2 A^2 + \dots + \alpha_{n-1} A^{n-1}$ for some scalars $\alpha_0, \dots, \alpha_{n-1}$).
8. Let A be an $n \times n$ Jordan block. Show that any matrix that commutes with A is a polynomial in A .
9. Let A be a square matrix whose minimal polynomial is equal to its characteristic polynomial. Show that if B is any matrix that commutes with A , then B is a polynomial in A .
10. Prove that an $n \times n$ complex matrix A is diagonalizable if and only if the minimal polynomial of A has distinct roots.
11. Let $G = \text{GL}_n(\mathbb{C})$ be the multiplicative group of invertible $n \times n$ matrices with complex entries and let g be an element of G of finite order. Show that g is diagonalizable.
12. Let V be a vector space and let $T : V \rightarrow V$ be a linear transformation.
 - (a) Show that T is invertible if and only if the minimal polynomial of T has non-zero constant term.
 - (b) Show that if T is invertible then T^{-1} can be expressed as a polynomial in T .

13. Let A and B be 5×5 complex matrices and suppose that A and B have the same eigenvectors. Show that if the minimal polynomial of A is $(x + 1)^2$ and the characteristic polynomial of B is x^5 , then $B^3 = 0$.
14. A square matrix A over \mathbb{C} is *Hermitian* if $\bar{A}^t = A$. Prove that the eigenvalues of a Hermitian matrix are all real.
15. (a) Prove that a 2×2 scalar matrix A over a field F has a square root (i.e., a matrix B satisfying $B^2 = A$).
- (b) Prove that a real symmetric matrix having the property that every negative eigenvalue occurs with even multiplicity has a square root. [Hint: Use (a).]
16. Let A and B be complex $n \times n$ matrices. Prove that if $AB = BA$, then A and B share a common eigenvector.
17. Let A be a 5×5 matrix with complex entries such that $A^3 = 0$. Find all possible Jordan Canonical Forms for A .
18. (a) Show that two 3×3 complex matrices are similar if and only if they have the same characteristic and minimal polynomials.
- (b) Is the conclusion of part (a) true for larger matrices? Prove or give a counter-example.
19. (a) Find all possible Jordan canonical forms of a 5×5 complex matrix with minimal polynomial $(x - 2)^2(x - 1)$.
- (b) Find all possible Jordan canonical forms of a complex matrix with characteristic polynomial $(x - 3)^3(x - 5)^2$.
20. Find all possible Jordan canonical forms for the following. EXPLAIN your answers.
- (a) A linear operator T with characteristic polynomial $\Delta(x) = (x - 2)^4(x - 3)^2$ and minimal polynomial $m(x) = (x - 2)^2(x - 3)^2$.
- (b) A linear operator T with characteristic polynomial $\Delta(x) = (x - 4)^5$ and such that $\dim \ker(T - 4I) = 3$.
21. A matrix A has characteristic polynomial $\Delta(x) = (x - 3)^5$ and minimal polynomial $m(x) = (x - 3)^3$.
- (a) List all possible Jordan canonical forms for A .
- (b) Determine the Jordan canonical form of the matrix

$$A = \begin{bmatrix} 3 & -1 & 2 & 0 & 0 \\ 2 & 3 & 0 & -2 & 0 \\ 1 & 0 & 3 & -1 & 0 \\ 0 & -1 & 2 & 3 & 0 \\ 0 & 2 & -3 & 0 & 3 \end{bmatrix}$$

which has the given characteristic and minimal polynomials.

22. Let $T : V \rightarrow V$ be a linear transformation defined on the finite dimensional vector space V . Let λ be an eigenvalue of T , and set $W_i = \{v \in V \mid (T - \lambda I)^i(v) = 0\}$. If m is the multiplicity of λ as a root of the characteristic polynomial of T , prove that $W_m = W_{m+1}$.

23. Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & -1 & 4 \\ 0 & 0 & 3 \end{bmatrix}$ be a matrix over the field F , where F is either the field of rational numbers or the field of p elements for some prime p .

(a) Find a basis of eigenvectors for A over those fields for which such a basis exists.

(b) What is the Jordan canonical form of A over the fields not included in part (a)?

24. Let $A = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, let $B = \begin{bmatrix} 1 & 1 & 0 & 0 \\ -1 & 3 & 0 & 0 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 3 \end{bmatrix}$, and let $C = \begin{bmatrix} 2 & -1 & 1 & -1 \\ 0 & 1 & 1 & -1 \\ 0 & -1 & 3 & -1 \\ 0 & 0 & 0 & 2 \end{bmatrix}$.

(a) Find the characteristic polynomial of A , B , and C .

(b) Find the minimal polynomial of A , B , and C .

(c) Find the eigenvalues of A , B , and C .

(d) Find the dimensions of all eigenspaces of A , B , and C .

(e) Find the Jordan canonical form of A , B , and C .

25. Let $A = \begin{bmatrix} 1 & 0 & a & b \\ 0 & 1 & 0 & 0 \\ 0 & c & 3 & -2 \\ 0 & d & 2 & -1 \end{bmatrix}$

(a) Determine conditions on a , b , c , and d so that there is only one Jordan block for each eigenvalue of A in the Jordan canonical form of A .

(b) Suppose now $a = c = d = 2$ and $b = -2$. Find the Jordan canonical form of A .

26. Let A be a square complex matrix with a single eigenvalue λ . Show that the number of blocks in the Jordan form of A is the dimension of the λ -eigenspace.

27. Let A be an $n \times n$ nilpotent matrix such that $A^{n-1} \neq 0$. Show that A has exactly one Jordan block.

28. Let $A = \begin{bmatrix} -1 & 4 & -2 \\ -2 & 5 & -2 \\ -1 & 2 & 0 \end{bmatrix}$ with characteristic polynomial $\Delta(x) = (x-1)^2(x-2)$.

(a) For each eigenvalue λ of A , find a basis for the eigenspace E_λ .

(b) Determine if A is diagonalizable. If so, give matrices P , B such that $P^{-1}AP = B$ and B is diagonal. If not, explain carefully *why* A is not diagonalizable.

29. Let $A = \begin{bmatrix} 2 & -1 & -1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{bmatrix}$.

(a) Verify that the characteristic polynomial of A is $\Delta(x) = x(x-1)^2$.

(b) For each eigenvalue λ of A , find a basis for the eigenspace E_λ .

(c) Determine if A is diagonalizable. If so, give matrices P , B such that $P^{-1}AP = B$ and B is diagonal. If not, explain carefully *why* A is not diagonalizable.

30. Let $A = \begin{bmatrix} 5 & 0 & 6 \\ 2 & 2 & 4 \\ -2 & 0 & -2 \end{bmatrix}$.

- (a) Verify that the characteristic polynomial of A is $\Delta(x) = (x - 1)(x - 2)^2$.
- (b) For each eigenvalue λ of A , find a basis for the eigenspace E_λ .
- (c) Determine if A is diagonalizable. If so, give matrices P, B such that $P^{-1}AP = B$ and B is diagonal. If not, explain carefully *why* A is not diagonalizable.

31. Let A be a matrix of the form $A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_1 & c_2 & c_3 & \cdots & c_n \end{bmatrix}$.

Show that the minimal polynomial and characteristic polynomial of A are equal.

Linear Transformations

- 32. (Fitting's Lemma for vector spaces) Let $\varphi : V \rightarrow V$ be a linear transformation of a finite dimensional vector space to itself. Prove that there exists a decomposition of V as $V = U \oplus W$ where each summand is φ -invariant, $\varphi|_U$ is nilpotent, and $\varphi|_W$ is nonsingular.
- 33. Let V be a vector space over a field F . A linear transformation $T : V \rightarrow V$ is said to be *idempotent* if $T^2 = T$. Prove that if T is idempotent then $V = V_0 \oplus V_1$, where $T(v_0) = 0$ for all $v_0 \in V_0$ and $T(v_1) = v_1$ for all $v_1 \in V_1$.
- 34. Let U, V and W be finite dimensional vector spaces with U a subspace of V . Show that if $T : V \rightarrow W$ is a linear transformation having the same rank as $T|_U : U \rightarrow W$, then U is complemented in V by a subspace K satisfying $T(x) = 0$ for all $x \in K$.
- 35. Let V and W be finite dimensional vector spaces and let $T : V \rightarrow W$ be a linear transformation. Show that $\dim(\ker T) + \dim(\text{Im } T) = \dim(V)$.
- 36. Let V be a finite dimensional vector space and $T : V \rightarrow V$ a *non-zero* linear operator. Show that if $\ker T = \text{Im } T$, then $\dim V$ is an *even* integer and the minimal polynomial of T is $m(x) = x^2$.
- 37. Let V be a finite dimensional vector space over a field F and let $T : V \rightarrow V$ be a nilpotent linear transformation. Show that the trace of T is 0.
- 38. Let $T : V \rightarrow W$ be a surjective linear transformation of finite dimensional vector spaces over a field F (acting on the left). Show that there is a linear transformation $S : W \rightarrow V$ such that $T \circ S$ is the identity map on W .
- 39. A linear transformation $T : V \rightarrow W$ is said to be independence preserving if $T(I) \subseteq W$ is linearly independent whenever $I \subseteq V$ is a linearly independent set. Show that T is independence preserving if and only if T is one-to-one.

40. Let $T : V \rightarrow W$ be a linear transformation of vector spaces over a field F .
- (a) Show that T is injective if and only if $\{T(v_1), \dots, T(v_n)\}$ is linearly independent in W whenever $\{v_1, \dots, v_n\}$ is linearly independent in V .
- (b) Show that T is surjective if and only if $\{T(x) \mid x \in X\}$ is a spanning set for W whenever X is a spanning set for V .
41. Let A be a complex $n \times n$ matrix, and let $L : \mathbb{C}^{n \times n} \rightarrow \mathbb{C}^{n \times n}$ be the linear transformation given by $L(M) = AM$ for $M \in \mathbb{C}^{n \times n}$. Express $\det L$ in terms of $\det A$ and prove your formula is correct.
42. Let A be a complex $n \times n$ matrix, and let $L : \mathbb{C}^{n \times n} \rightarrow \mathbb{C}^{n \times n}$ be the linear transformation given by $L(X) = AX + XA$ for $X \in \mathbb{C}^{n \times n}$. Prove that if A is a nilpotent matrix, then L is a nilpotent operator.
43. Let $T : V \rightarrow V$ be a linear transformation. Let $X = \ker T^{n-2}$, $Y = \ker T^{n-1}$, and $Z = \ker T^n$. Observe that $X \subseteq Y \subseteq Z$ (you need not prove this). Suppose

$$\{u_1, \dots, u_r\}, \{u_1, \dots, u_r, v_1, \dots, v_s\}, \{u_1, \dots, u_r, v_1, \dots, v_s, w_1, \dots, w_t\}$$

are bases for X, Y, Z , respectively. Show that $S = \{u_1, \dots, u_r, T(w_1), \dots, T(w_t)\}$ is contained in Y and is linearly independent.

Vector Spaces

44. Let $\{v_1, v_2, \dots, v_n\}$ be a basis for a vector space V over \mathbb{R} . Show that if w is any vector in V , then for some choice of sign \pm , $\{v_1 \pm w, v_2, \dots, v_n\}$ is a basis for V .
45. Let V be a finite dimensional vector space over the field F . Let V^* be the dual space of V (that is, V^* is the vector space of linear transformations $T : V \rightarrow F$). Show that $V \cong V^*$.
46. Let V be a vector space over the field F . Let V^* be the dual space of V and let V^{**} be the dual space of V^* . Show that there is an injective linear transformation $\varphi : V \rightarrow V^{**}$.
47. Let V be a finite dimensional vector space and let W be a subspace. Show that $\dim V/W = \dim V - \dim W$.
48. Let V be a vector space and let U and W be finite dimensional subspaces of V . Show that $\dim(U + W) = \dim U + \dim W - \dim U \cap W$.
49. Let V be a finite-dimensional vector space over a field F and let U be a subspace. Show that there is a subspace W of V such that $V = U \oplus W$.
50. Let V be the vector space of $n \times n$ matrices over the field \mathbb{R} of real numbers. Let U be the subspace of V consisting of symmetric matrices and W the subspace of V consisting of skew-symmetric matrices. Show that $V = U \oplus W$.
51. Let V be the vector space over the field \mathbb{R} of real numbers consisting of all functions from \mathbb{R} into \mathbb{R} . Let U be the subspace of even functions and W the subspace of odd functions. Show that $V = U \oplus W$.

52. Let U , V , and W be vector spaces over a field F and let $S : U \rightarrow V$ and $T : V \rightarrow W$ be linear transformations such that $T \circ S = \mathbf{0}$, the zero map. Show that

$$\dim(W/\text{Im } T) - \dim(\ker T/\text{Im } S) + \dim \ker S = \dim W - \dim V + \dim U.$$

53. Let A , B , and C be subspaces of the nonzero vector space V satisfying

$$V = A \oplus B = B \oplus C = A \oplus C.$$

Show that there exists a 2-dimensional subspace $W \subseteq V$ such that each of $W \cap A$, $W \cap B$, and $W \cap C$ has dimension 1.

54. Let

$$V_{-1} = 0 \xrightarrow{L_{-1}=0} V_0 \xrightarrow{L_0} V_1 \xrightarrow{L_1} \dots \xrightarrow{L_{n-1}} V_n \xrightarrow{L_n=0} V_{n+1} = 0$$

be a sequence of finite dimensional vector spaces and linear transformations with $L_{i+1} \circ L_i = 0$ for all $i = 0, \dots, n$. Therefore, the quotients $H_i = \ker(L_i)/\text{im}(L_{i-1})$ are defined for $0 \leq i \leq n$.

Prove that $\sum_i (-1)^i \dim V_i = \sum_i (-1)^i \dim H_i$.

55. If V is a finite dimensional vector space, let V^* denote the dual of V . If (\cdot, \cdot) is a non-degenerate bilinear form on V , and W is a subspace of V , define $W^\perp = \{v \in V \mid (v, w) = 0 \text{ for all } w \in W\}$. Show that if X and Y are subspaces of V with $Y \subseteq X$, then $X^\perp \subseteq Y^\perp$ and $Y^\perp/X^\perp \cong (X/Y)^*$.

Inner Product Spaces

56. Let (\cdot, \cdot) be a positive definite inner product on the finite dimensional real vector space V . Let $S = \{v_1, v_2, \dots, v_k\}$ be a set of vectors satisfying $(v_i, v_j) < 0$ for all $i \neq j$. Prove that $\dim(\text{span } S) \geq k - 1$.
57. Let $\{v_1, v_2, \dots, v_k\}$ be a linearly independent set of vectors in the real inner product space V . Show that there exists a unique set $\{u_1, u_2, \dots, u_k\}$ of vectors with the property that $(u_i, v_i) > 0$ for all i , and $\{u_1, u_2, \dots, u_i\}$ is an orthonormal basis for $\text{Span}\{v_1, v_2, \dots, v_i\}$ for every i .
58. Let (\cdot, \cdot) be a Hermitian inner product defined on the complex vector space V . If $\varphi : V \rightarrow V$ is a normal operator ($\varphi \circ \varphi^* = \varphi^* \circ \varphi$, where φ^* is the adjoint of φ), prove that V contains an orthonormal basis of eigenvectors for φ .

Modules

59. Let M be a nonzero R -module with the property that every R -submodule N is complemented (that is, there exists another R -submodule C such that $M = N + C$ and $N \cap C = \{0\}$). Give a direct proof that M contains simple submodules.
60. Let $R = F^{n \times n}$ be the ring of $n \times n$ matrices over a field F . Prove that the (right) R -module $F^{1 \times n}$, consisting of the row space of $1 \times n$ matrices, is the unique simple R -module (up to isomorphism).
61. Let $R \subseteq S$ be an inclusion of rings (sharing the same identity element). Let S_R be the right R -module where the module action is right multiplication. Assume S_R is isomorphic to a direct sum of n copies of R . Prove that S is isomorphic to a subring of $M_n(R)$, the ring of $n \times n$ matrices over R .

62. Let M be a module over a ring R with identity, and assume that M has finite composition length. If $\varphi : M \rightarrow M$ is an R -endomorphism of M , prove that M decomposes as a direct sum of R -submodules $M = U \oplus W$ where each summand is φ -invariant, $\varphi|_U$ is nilpotent, and $\varphi|_W$ is an automorphism.
63. Let R be a ring with identity, and let I be a right ideal of R which is a direct summand of R (i.e., $R = I \oplus J$ for some right ideal J). Prove that if M is any R -module, and $\varphi : M \rightarrow I$ is any surjective R -homomorphism, then there exists an R -homomorphism $\psi : I \rightarrow M$ satisfying $\varphi \circ \psi = 1|_I$.
64. Let M be an R -module and let N be an R -submodule of M . Prove that M is Noetherian if and only if both N and M/N are Noetherian.
65. Let M be an R -module and let N be an R -submodule of M . Prove that M is Artinian if and only if both N and M/N are Artinian.
66. Let M be an R -module, where R is a ring. Prove that the following statements about M are equivalent.
- (i) M is a sum (not necessarily direct) of simple submodules.
 - (ii) M is a direct sum of certain simple submodules.
 - (iii) For every submodule N of M , there exists a complement (i.e., a submodule C such that $M = N + C$ and $N \cap C = 0$).
67. Let R be a ring and let M be a simple R -module. Let $D = \text{End}_R(M)$ be the ring of R -endomorphisms of M (under composition and pointwise addition). Prove that D is a division ring.
68. Let M be an R -module that is generated by finitely many simple submodules. Prove that M is a direct sum of finitely many simple R -modules.

GROUP THEORY

General Group Theory

1. Prove or give a counter-example:
 - (a) If H_1 and H_2 are groups and $G = H_1 \times H_2$, then any subgroup of G is of the form $K_1 \times K_2$, where K_i is a subgroup of H_i for $i = 1, 2$.
 - (b) If $H \trianglelefteq N$ and $N \trianglelefteq G$ then $H \trianglelefteq G$.
 - (c) If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$.
 - (d) If $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$ with $N_1 \cong N_2$ and $G_1/N_1 \cong G_2/N_2$, then $G_1 \cong G_2$.
 - (e) If $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$ with $G_1 \cong G_2$ and $N_1 \cong N_2$, then $G_1/N_1 \cong G_2/N_2$.
 - (f) If $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$ with $G_1 \cong G_2$ and $G_1/N_1 \cong G_2/N_2$, then $N_1 \cong N_2$.
2. Let G be a group and let N be a normal subgroup of index n . Show that $g^n \in N$ for all $g \in G$.
3. Let G be a group. A subgroup H of G is called a *characteristic* subgroup of G if $\varphi(H) = H$ for every automorphism φ of G . Show that if H is a characteristic subgroup of N and N is a normal subgroup of G , then H is a normal subgroup of G .
4. Show that if H is a characteristic subgroup of N and N is a characteristic subgroup of G , then H is a characteristic subgroup of G .
5. Let G be a finite group, H a subgroup of G and N a normal subgroup of G . Show that if the order of H is relatively prime to the index of N in G , then $H \subseteq N$.
6. Let G be a group and let $Z(G)$ be its center. Show that if $G/Z(G)$ is cyclic, then G is abelian.
7. Let G be a group and let $Z(G)$ be the center of G . Prove or disprove the following.
 - (a) If $G/Z(G)$ is cyclic, then G is abelian.
 - (b) If $G/Z(G)$ is abelian, then G is abelian.
 - (c) If G is of order p^2 , where p is a prime, then G is abelian.
8. Show that if G is a nonabelian finite group, then $|Z(G)| \leq \frac{1}{4}|G|$.
9. Let G be a finite group and let M be a maximal subgroup of G . Show that if M is a normal subgroup of G , then $|G : M|$ is prime.
10. Show that if \mathcal{K} and \mathcal{L} are conjugacy classes of groups G and H , respectively, then $\mathcal{K} \times \mathcal{L}$ is a conjugacy class of $G \times H$.
11.
 - (a) State a formula relating orders of centralizers and cardinalities of conjugacy classes in a finite group G .
 - (b) Let G be a finite group with a proper normal subgroup N that is not contained in the center of G . Prove that G has a proper subgroup H with $|H| > |G|^{1/2}$. [Hint: (a) applied to a noncentral element of G inside N is useful.]
12. Let H be a subgroup of G of index 2 and let g be an element of H . Show that if $C_G(g) \subseteq H$ then the conjugacy class of g in G splits into 2 conjugacy classes in H , and if $C_G(g) \not\subseteq H$, then the class of g in G remains the class of g in H .

13. Let G be a finite group, H a subgroup of G of index 2, and $x \in H$. Denote by $cl_G(x)$ the conjugacy class of x in G and by $cl_H(x)$ the conjugacy class of x in H .
- (a) Show that if $C_G(x) \leq H$, then $|cl_H(x)| = \frac{1}{2}|cl_G(x)|$.
- (b) Show that if $C_G(x)$ is not contained in H , then $|cl_H(x)| = |cl_G(x)|$.
- [Hint: Consider centralizer orders.]
14. Let N be a normal subgroup of G and let \mathcal{C} be a conjugacy class of G that is contained in N . Prove that if $|G : N| = p$ is prime, then either \mathcal{C} is a conjugacy class of N or \mathcal{C} is a union of p distinct conjugacy classes of N .
15. Let G be a group, $g \in G$ an element of order greater than 2 (possibly infinite) such that the conjugacy class of g has an odd number of elements. Prove that g is not conjugate to g^{-1} .
16. Let H be a subgroup of the group G . Show that the following are equivalent:
- (i) $x^{-1}y^{-1}xy \in H$ for all $x, y \in G$
- (ii) $H \trianglelefteq G$ and G/H is abelian.
17. Let H and K be subgroups of a group G , with $K \trianglelefteq G$ and $K \leq H$. Show that H/K is contained in the center of G/K if and only if $[H, G] \leq K$ (where $[H, G] = \langle h^{-1}g^{-1}hg \mid h \in H, g \in G \rangle$).
18. Let G be any group for which G'/G'' and G''/G''' are cyclic. Prove that $G'' = G'''$.
19. Let $GL_n(\mathbb{C})$ be the group of invertible $n \times n$ matrices with complex entries. Give a complete list of conjugacy class representatives for $GL_2(\mathbb{C})$ and for $GL_3(\mathbb{C})$.
20. Let H be a subgroup of the group G and let T be a set of representatives for the distinct right cosets of H in G . In particular, if $t \in T$ and $g \in G$ then tg belongs to a unique coset of the form Ht' for some $t' \in T$. Write $t' = t \cdot g$. Prove that if $S \subseteq G$ generates G , then the set $\{ts(t \cdot s)^{-1} \mid t \in T, s \in S\}$ generates H .
- Suggestion: If K denotes the subgroup generated by this set, prove the stronger assertion that $KT = G$. Start by showing that KT is stable under right multiplication by elements of G .
21. Let G be a group, H a subgroup of finite index n , G/H the set of left cosets of H in G , and $S(G/H)$ the group of permutations of G/H (with composition from right to left). Define $f : G \rightarrow S(G/H)$ by $f(g)(xH) = (gx)H$ for $g, x \in G$.
- (a) Show that f is a group homomorphism.
- (b) Show that if H is a normal subgroup of G , then H is the kernel of f .
22. Let G be an abelian group. Let $K = \{a \in G : a^2 = 1\}$ and let $H = \{x^2 : x \in G\}$. Show that $G/K \cong H$.
23. Let $N \trianglelefteq G$ such that every subgroup of N is normal in G and $C_G(N) \subseteq N$. Prove that G/N is abelian.
24. Let H be a subgroup of G having a normal complement (i.e., a normal subgroup N of G satisfying $HN = G$ and $H \cap N = \langle 1 \rangle$). Prove that if two elements of H are conjugate in G , then they are conjugate in H .

25. Let H be a subgroup of the group G with the property that whenever two elements of G are conjugate, then the conjugating element can be chosen within H . Prove that the commutator subgroup G' of G is contained in H .
26. Let $a \in G$ be fixed, where G is a group. Prove that a commutes with each of its conjugates in G if and only if a belongs to an abelian normal subgroup of G .
27. Show that if H and K are subgroups of a finite group G satisfying $(|G : H|, |G : K|) = 1$, then $G = HK$.
28. Let $G = A \times B$ be a direct product of the subgroups A and B . Suppose H is a subgroup of G that satisfies $HA = G = HB$ and $H \cap A = \langle 1 \rangle = H \cap B$. Prove that A is isomorphic to B .
29. Let N_1, N_2 , and N_3 be normal subgroups of a group G and assume that for $i \neq j$, $N_i \cap N_j = \langle 1 \rangle$ and $N_i N_j = G$. Show that G is isomorphic to $N_1 \times N_2$ and G is abelian.
30. Show that if the size of each conjugacy class of a group G is at most 2, then $G' \leq Z(G)$.
31. Let N be a normal subgroup of G . Show that if $N \cap G' = \langle 1 \rangle$, then N is contained in the center of G .
32. Let G be a finite group.
 - (a) Show that every proper subgroup of G is contained in a maximal subgroup.
 - (b) Show that the intersection of all maximal subgroups of G is a normal subgroup.
33. Let G be a group. Show that G has a composition series if and only if G satisfies the following two conditions:
 - (i) If $G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots$ is any subnormal series, then there is an n such that $H_n = H_{n+1} = \cdots$.
 - (ii) If H is any subgroup of G in a subnormal series and $K_1 \leq K_2 \leq K_3 \leq \cdots$ is an ascending chain of normal subgroups of H , then there is an m such that $K_m = K_{m+1} = \cdots$.

Cyclic Groups

34. Let φ be the Euler φ -function — that is, $\varphi(n)$ is the number of positive integers less than the integer n and relatively prime to n . Let G be a finite group of order n with at most d elements x satisfying $x^d = 1$ for each divisor d of n .
 - (a) Show that in a *cyclic* group of order n , the number of elements of order d is $\varphi(d)$ for each divisor d of n . Deduce that $\sum_{d|n} \varphi(d) = n$.
 - (b) Let $\psi(d)$ be the number of elements of G of order d . Show that for any d , either $\psi(d) = 0$ or $\psi(d) = \varphi(d)$.
 - (c) Show that G is cyclic.
 - (d) Show that any finite subgroup of the multiplicative group of a field must be cyclic.
35. Show that if G is a cyclic group then every subgroup of G is cyclic.
36. Show that if G is a finite cyclic group, then G has exactly one subgroup of order m for each positive integer m dividing $|G|$.

37. Show that if H is a cyclic normal subgroup of a finite group G , then every subgroup of H is a normal subgroup of G .
38. Let G be a cyclic group of order 12 with generator a . Find b in G such that $G/\langle b \rangle$ is isomorphic to $\langle a^{10} \rangle$. (Here $\langle x \rangle$ denotes the subgroup of G generated by $\{x\}$, for $x \in G$.)

Homomorphisms

39. State and prove the three “isomorphism theorems” (for groups).
40. Let G be a group and let K be a subgroup of G . Give necessary and sufficient conditions for K to be the kernel of a homomorphism from G to G . Prove your answer. (*N.B.*: The homomorphism must be from G to G .)
41. Let G be a group with a normal subgroup N of order 5, such that $G/N \cong S_3$. Show that $|G| = 30$, G has a normal subgroup of order 15, and G has 3 subgroups of order 10 that are not normal.
42. Let G be a group with a normal subgroup N of order 7, such that $G/N \cong D_{10}$, the dihedral group of order 10. Show that $|G| = 70$, G has a normal subgroup of order 35, and G has 5 subgroups of order 14 that are not normal.
43. Let $f : G \rightarrow H$ be a homomorphism of groups with kernel K and image I .
- (a) Show that if N is a subgroup of G then $f^{-1}(f(N)) = KN$.
- (b) Show that if L is a subgroup of H then $f(f^{-1}(L)) = I \cap L$.
44. Let G and H be finite groups with $(|G|, |H|) = 1$. Show that if $\varphi : G \rightarrow H$ is a homomorphism, then $\varphi(g) = 1_H$ for all g in G (where 1_H is the identity element of H).
45. Let $G = \text{GL}_n(\mathbb{R})$ be the (multiplicative) group of nonsingular $n \times n$ matrices with real entries and let $S = \text{SL}_n(\mathbb{R})$ be the subgroup of G consisting of matrices of determinant 1. Show that $S \trianglelefteq G$ and $G/S \cong \mathbb{R}^*$, the multiplicative group of real numbers.
46. (a) Suppose H and K are normal subgroups of a group G . Show that there exists a one-to-one homomorphism

$$\varphi : G/H \cap K \rightarrow G/H \times G/K.$$

- (b) Use part (a) to show that if $(m, n) = 1$ then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
47. Prove that the commutator subgroup of $\text{SL}_2(\mathbb{Z})$ is *proper* in $\text{SL}_2(\mathbb{Z})$. (Hint: Any homomorphism of rings $R \rightarrow S$ induces a homomorphism of groups $\text{SL}_2(R) \rightarrow \text{SL}_2(S)$.)
48. Let H and K be subgroups of a finite group G and assume H is isomorphic to K . Prove that there exists a group \tilde{G} containing G as a subgroup, such that H and K are conjugate in \tilde{G} .

Automorphism Groups

49. Let $\text{Inn}(G)$ be the group of inner automorphisms of the group G and let $\text{Aut}(G)$ be the full automorphism group.
- (a) Show that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$.
- (b) Show that if $Z(G)$ is the center of G , then $\text{Inn}(G) \cong G/Z(G)$.

50. Show that if H is a subgroup of G , then $C_G(H) \trianglelefteq N_G(H)$ and $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.
51. Let G be a simple group of order greater than 2 and let $\text{Aut}(G)$ be its automorphism group. Show that the center of $\text{Aut}(G)$ is trivial if and only if G is non-abelian.
52. Let G be a finite group with a normal subgroup $N \cong S_3$. Show that there is a subgroup H of G such that $G = N \times H$.
53. A group N is said to be *complete* if the center of N is trivial and every automorphism of N is inner. Show that if G is a group, $N \trianglelefteq G$, and N is complete, then $G = N \times C_G(N)$.

Abelian Groups

54. Let A be an abelian group with the following property:
 (*) If $B \leq A$ then there is a $C \leq A$ with $A = B \oplus C$.
 Show the following.
- (a) Each subgroup of A satisfies (*).
 (b) Each element of A has finite order.
 (c) If p is a prime, then A has no element of order p^2 .
55. Let A be an abelian p -group of exponent p^m . Show that if B is a subgroup of A of order p^m and both B and A/B are cyclic, then there is a subgroup C of A such that $A = B + C$ and $B \cap C = \{0\}$.
56. (a) List all abelian groups of order 360 (up to isomorphism).
 (b) Find the invariant factors and elementary divisors of the group

$$G = \mathbb{Z}_{25} \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{48} \oplus \mathbb{Z}_{300}.$$

57. Consider the property (*) of abelian groups G :

(*) If H is any subgroup of G then there exists a subgroup F of G such that $G/H \cong F$.

Show that if G is a finitely generated abelian group then G has property (*) if and only if G is finite.

58. Let n be a positive integer and let $A = \mathbb{Z}^n$. Prove that if B is any subgroup of A that is generated by fewer than n elements, then the index $[A : B]$ is infinite.
59. Show that if A , B , and C are abelian groups, then

$$\text{Hom}(A, B \oplus C) \cong \text{Hom}(A, B) \oplus \text{Hom}(A, C).$$

60. Show that if A , B , and C are abelian groups, then

$$\text{Hom}(A \oplus B, C) \cong \text{Hom}(A, C) \oplus \text{Hom}(B, C).$$

61. Let A, B, A_α ($\alpha \in I$) and B_β ($\beta \in J$) be abelian groups. Prove the following:

$$\text{Hom}\left(\bigoplus_{\alpha \in I} A_\alpha, B\right) \cong \prod_{\alpha \in I} \text{Hom}(A_\alpha, B)$$

$$\text{Hom}\left(A, \prod_{\beta \in J} B_\beta\right) \cong \prod_{\beta \in J} \text{Hom}(A, B_\beta).$$

62. Let:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & E & \longrightarrow & 0 \\ & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \delta \downarrow & & \epsilon \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & E' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of Abelian groups and homomorphisms in which both rows are exact. If $\alpha, \beta, \delta,$ and ϵ are isomorphisms, prove that γ is an isomorphism also.

63. Let $A, U, V, W, X,$ and Y be abelian groups.

If $\alpha \in \text{Hom}(X, Y)$ define $\alpha_* : \text{Hom}(A, X) \rightarrow \text{Hom}(A, Y)$ by $\alpha_*(f) = \alpha \circ f$. If

$$0 \rightarrow U \xrightarrow{\alpha} V \xrightarrow{\beta} W \rightarrow 0$$

is exact, to what extent is

$$0 \rightarrow \text{Hom}(A, U) \xrightarrow{\alpha_*} \text{Hom}(A, V) \xrightarrow{\beta_*} \text{Hom}(A, W) \rightarrow 0$$

exact? Prove your assertions.

64. Same as the previous problem, except use $\text{Hom}(-, A)$ instead, making the obvious modifications.

Symmetric Groups

65. (a) Find the centralizer in S_7 of $(1\ 2\ 3)(4\ 5\ 6\ 7)$.
 (b) How many elements of order 12 are there in S_7 ?
66. (a) Give an example of two nonconjugate elements of S_7 that have the same order.
 (b) If $g \in S_7$ has maximal order, what is $o(g)$?
 (c) Does the element g that you found in part (b) lie in A_7 ?
 (d) Is the set $\{h \in S_7 \mid o(h) = o(g)\}$ a single conjugacy class in S_7 , where g is the element found in part (b)?
67. (a) Give a representative for each conjugacy class of elements of order 6 in S_6 .
 (b) Find the order of the centralizer in S_6 of each element from part (a).
68. How many elements of order 6 are there in S_6 ? How many in A_6 ?
69. (a) Write $\sigma = (4\ 5\ 6)(2\ 3)(1\ 2)(6\ 7\ 8)$ as a product of disjoint cycles and find the order of σ .
 (b) Let $n > 1$ be an odd integer. Show that S_n has an element of order $2(n-2)$.

70. Let $\sigma = (1\ 2\ 3)(4\ 5\ 6) \in S_6$.
- Determine the size of the conjugacy class of σ and the order of the centralizer of σ in S_6 .
 - Determine if $C_{S_6}(\sigma)$ is abelian or non-abelian. Prove your answer.
71. Let G be a subgroup of the symmetric group S_n . Show that if G contains an odd permutation then $G \cap A_n$ is of index 2 in G .
72. Show that if G is a non-abelian simple subgroup of S_n , then G is contained in A_n .
73. Show that if G is a subgroup of S_n of index 2, then $G = A_n$.
74. For $i = 1, \dots, n-1$, let x_i be the transposition $(i\ i+1)$ in the symmetric group S_n . Show that $S_n = \langle x_1, \dots, x_{n-1} \rangle$.
75. Let H be a subgroup of S_n . Show that if H is a transitive subgroup of S_n and H is generated by some set of transpositions, then $H = S_n$.
76. Prove that the symmetric group S_n is a maximal subgroup of S_{n+1} .
[Hint: Show that if $g \in S_{n+1} - S_n$, then $S_{n+1} = S_n \cup S_n g S_n$.]
77. (a) If $n = k + \ell$ with $k \neq \ell$, then $S_k \times S_\ell$ is a maximal subgroup of S_n in the natural embedding.
(b) If $n = 2k$, then $S_k \times S_k$ is not a maximal subgroup of S_n in the natural embedding.
78. (a) Prove that if A is a transitive abelian subgroup of the symmetric group S_n , then $|A| = n$.
(b) Give an example of n , A_1 , A_2 , where A_1 and A_2 are transitive abelian subgroups of S_n , but A_1 is not isomorphic to A_2 .
79. Let A be an abelian, transitive subgroup of S_n . Show that for all $\alpha \in \{1, \dots, n\}$, the stabilizer A_α of α in A is trivial.
80. Let H be a subgroup of index n in a group G . Let S_n be the symmetric group on n letters and let $S_{n-1} \subseteq S_n$ be the usual embedding. Show that $H = f^{-1}(S_{n-1})$ for some homomorphism $f : G \rightarrow S_n$. (Hint: Let G act on the cosets of H .)
81. Show that if $\sigma = \rho\lambda \in S_{m+n}$ is the product of an m -cycle ρ and an n -cycle λ , with ρ and λ disjoint and $m \neq n$, then the centralizer in S_{m+n} of σ is $\langle \rho, \lambda \rangle$.
82. Let τ be an element of the symmetric group S_n and let $\sigma \in S_n$ be a transposition. Show that the number of cycles in the cycle decomposition of $\sigma\tau$ is either one more or one less than the number of cycles in the cycle decomposition of τ .
83. Show that if $\sigma \in S_n$ is an $(n-1)$ -cycle, where $n \geq 3$, then $C(\sigma) = \langle \sigma \rangle$.

Infinite Groups

84. Let A and B be subgroups of the additive group of rationals \mathbb{Q} . Show that if A is isomorphic to B and $f : A \rightarrow B$ is an isomorphism, then there exists $q \in \mathbb{Q}$ such that $f(x) = qx$ for all $x \in A$.
85. (a) Prove that the additive group of the rational numbers is not cyclic.
(b) Prove that a finitely generated subgroup of the additive group of the rational numbers must be cyclic.

86. If G is a finitely generated group and n is a positive integer, prove that there are at most finitely many subgroups of index n in G . (HINT: Consider maps into the symmetric group S_n .)
87. Let G be a group with a proper subgroup of finite index. Show that G has a proper normal subgroup of finite index.
88. Let \mathbb{Q} be the additive group of rationals and \mathbb{Z} its subgroup of integers. Prove the following.
- If n is a positive integer, then \mathbb{Q}/\mathbb{Z} has an element of order n .
 - If n is a positive integer, then \mathbb{Q}/\mathbb{Z} has a unique subgroup of order n .
 - Every finite subgroup of \mathbb{Q}/\mathbb{Z} is cyclic.
89. Let G have the presentation $G = \langle a, b \mid a^2 = 1, a^{-1}bab = 1 \rangle$. Prove that G is infinite but the commutator subgroup of G is of finite index in G .
90. Let N be a normal subgroup of G with the order of N finite. Prove there is a normal subgroup M of G such that $[G : M]$ is finite and $nm = mn$ for all $n \in N$ and $m \in M$.
91. Let G be a finitely presented group in which there are fewer relations than generators. Prove that G is necessarily infinite.

p -Groups

92. Show that the center of a finite p -group is non-trivial.
93. Show that if P is a finite p -group and $\langle 1 \rangle \neq N \trianglelefteq P$, then $N \cap Z(P) \neq \langle 1 \rangle$.
94. Let P be a finite p -group and let H be a proper subgroup of P . Prove that H is a proper subgroup of its normalizer $N_P(H)$.
95. Show that a group of order p^2 , where p is a prime, must be abelian.
96. Let p be a prime and let G be a non-abelian group of order p^3 .
- Show that the center $Z(G)$ of G and the commutator subgroup of G are equal and of order p .
 - Show that $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.
97. Let p be a prime and let G be a group of order p^n satisfying the following property:
 (*) If A and B are subgroups of G then $A \leq B$ or $B \leq A$.
 Prove that G is a cyclic group.
98. Let G be a finite group. Prove that G is a cyclic p -group, for some prime p , if and only if G has exactly one conjugacy class of maximal subgroups.
99. Let G be a finite p -group for some prime p . Show that if G is not cyclic, then G has at least $p + 1$ maximal subgroups.
100. Let P be a finite p -group in which all the non-identity elements of the center $Z(P)$ have order p . If $\{Z_i(P)\}$ is the upper central series of P , prove that for every i , every non-identity element of $Z_{i+1}(P)/Z_i(P)$ has order p .
101. Let P be a p -group satisfying $[P : Z(P)] = p^n$. Show that $|P'| \leq p^{\frac{n(n-1)}{2}}$.
 (Hint: Use induction on n . Apply the inductive hypothesis to a maximal subgroup of P .)

102. Let G be a group of order 16 with an element g of order 4. Prove that the subgroup of G generated by g^2 is normal in G .

Group Actions

103. Show that if the center of a group G is of index n in G , then every conjugacy class of G has at most n elements.
104. Let $G_n = \text{GL}_n(\mathbb{C})$ be the group of invertible $n \times n$ matrices with complex entries and let $M_n = M_n(\mathbb{C})$ be the set of all $n \times n$ complex matrices.
- (a) Show that for $g \in G_n$ and $m \in M_n$, $g \cdot m = gm g^{-1}$ defines a (left) action of G_n on M_n .
- (b) For $n = 2$ and $n = 3$, find a complete set of orbit representatives.
105. Let G be a finite group acting on a set A and suppose that for any two ordered pairs (a_1, a_2) and (b_1, b_2) of elements of A , there is an element $g \in G$ such that $g \cdot a_i = b_i$ for $i = 1, 2$. Show that if $|A| = n$, then $|G|$ is divisible by $n(n - 1)$. [Hint: Show that if $a \in A$ then G_a acts transitively on $A - \{a\}$.]
106. Let G be a group acting on a set Ω . Show that the following are equivalent.
- (i) The action is doubly transitive (i.e., for any two ordered pairs $(\alpha_1, \beta_1), (\alpha_2, \beta_2)$ of elements of Ω with $\alpha_1 \neq \beta_1$ and $\alpha_2 \neq \beta_2$, there is an element g in G such that $g \cdot \alpha_1 = \alpha_2$ and $g \cdot \beta_1 = \beta_2$).
- (ii) For all $\alpha \in \Omega$, the stabilizer G_α acts transitively on $\Omega - \{\alpha\}$.
107. Let G be a group acting transitively on the set Ω . Show that if $\alpha \neq \beta$ are elements of Ω , then $G_\alpha G_\beta$ is a proper subset of G .
108. Let G be a group acting transitively on a set A . Show that if there is an element $a \in A$ such that $G_a = \{1\}$, then $G_b = \{1\}$ for all $b \in A$.
109. Let the group G act transitively on the set Ω , and let N be a normal subgroup of G . Prove that G permutes the N -orbits of Ω and that these orbits all have the same size.
110. Let G act on a set A and let B be a subset of A . For $g \in G$, let $g \cdot B = \{g \cdot b : b \in B\}$. Show that $H = \{g \in G : g \cdot B = B\}$ is a subgroup of G .
111. Let G be a group acting on the set S and let H be a subgroup of G acting transitively on S . Show that if $t \in S$ then $G = G_t H$, where G_t is the stabilizer of t in G .
112. Let G be a finite group. Show that if G has a normal subgroup N of order 3 that is not contained in the center of G , then G has a subgroup of index 2. [Hint: The group G acts on N by conjugation.]
113. (a) Let G be a finite group acting on the finite set S . For $g \in G$, let

$$F(g) = |\{x \in S : g \cdot x = x\}|.$$

Show that the number of orbits is $\frac{1}{|G|} \sum_{g \in G} F(g)$.

- (b) Show that the number of conjugacy classes of a finite group G is $\frac{1}{|G|} \sum_{g \in G} |C_G(g)|$.

114. Let G be a subgroup of S_n that acts transitively on $\{1, 2, \dots, n\}$.
- Show that if $G_1 = \{g \in G \mid g \cdot 1 = 1\}$ then $[G : G_1] = n$.
 - Show that if G is abelian then G is of order n .
115. Let G be a finite group acting transitively on a set Ω . Fix $\alpha \in \Omega$ and let G_α be the stabilizer of α in G . Let Δ be the set of points fixed by G_α , i.e. $\Delta = \{\beta \in \Omega \mid \beta \cdot x = \beta \forall x \in G_\alpha\}$. Show that Δ is stabilized by $N_G(G_\alpha)$ and that $N_G(G_\alpha)$ acts transitively on Δ .
116. Let G act transitively on a set Ω , fix $\alpha \in \Omega$, and let $H = G_\alpha$. Show that the orbits of H on Ω are in one-to-one correspondence with the $H - H$ double cosets in G .
117. Let G act on a set Ω and assume N is a normal subgroup of G that is contained in the kernel of the action. Show that there is a natural action of G/N on Ω which satisfies the property that G is transitive if and only if G/N is transitive.
118. Let G be a group with a subgroup H of finite index n . Show that there is a homomorphism $\varphi : G \rightarrow S_n$ with $\ker \varphi \subseteq H$.
119. Suppose a group G has a subgroup H with $|G : H| = n < \infty$. Prove that G has a normal subgroup N with $N \subseteq H$ and $|G : N| \leq n!$.
120. Let $n > 1$ be a fixed integer. Prove that there are only finitely many simple groups (up to isomorphism) containing a proper subgroup of index less than or equal to n .
121. Let $n = p^m r$ where p is prime and r is an integer greater than 1 such that p does not divide r . Show that if there is a simple group of order n , then p^m divides $(r - 1)!$.
122. Show that if G is a simple group of order greater than 60, then G has no proper subgroup of index less than or equal to 5.
123. Let G be a finite simple group containing an element of order 21. Show that every proper subgroup of G has index at least 10.
124. Let G be a finite group and let K be a subgroup of index p , where p is the smallest prime dividing the order of G . Show that K is a normal subgroup of G .
125. Let G be a nonabelian finite simple group and let H be a subgroup of index p , where p is a prime. Prove that the number of distinct conjugates of H in G is p .
126. Let G be a finite simple group with a subgroup H of prime index p . Show that p must be the largest prime dividing the order of G .
127. Let G be a finite simple group and p a prime such that p^2 divides the order of G . Show that G has no subgroup of index p .
128. Let G be a finite group in which a Sylow 2-subgroup is cyclic. Prove that there exists a normal subgroup N of odd order such that the index $[G : N]$ is a power of 2. [Hint: Generalize the previous problem.]

129. (a) Let G be a subgroup of the symmetric group S_n . Show that if G contains an odd permutation then $G \cap A_n$ is of index 2 in G .
- (b) Let G be a group of order $2r$, where $r > 1$ is an odd integer. Show that in the regular permutation representation of G , an element t of G of order 2 corresponds to an odd permutation.
- (c) Show that a group of order $2r$, with $r > 1$ an odd integer, cannot be simple.
130. Let G be a finite cyclic group and H a subgroup of index p , p a prime. Suppose G acts on a set S and the restriction of the action to H is transitive. Let G_x, H_x be the stabilizer of $x \in S$ in G, H , respectively. Show the following.
- (a) $H_x = G_x \cap H$
- (b) $[H : H_x] = [G : G_x] = |S|$
- (c) $|S|$ is not divisible by p .
131. Let G be a finite group and p a prime. Then G acts on $\text{Syl}_p(G)$ by conjugation; let $\rho : G \rightarrow \text{Sym}(\text{Syl}_p(G))$ be the homomorphism corresponding to this action.
- (a) $\rho(P)$ fixes exactly one point (element of $\text{Syl}_p(G)$).
- (b) If $P \in \text{Syl}_p(G)$ has order p , then $\rho(x)$ is a product of one 1-cycle and a certain number of p -cycles, for $x \in P - \{1\}$.
- (c) If $P \in \text{Syl}_p(G)$ has order p and $y \in N_G(P) - C_G(P)$ then $\rho(y)$ fixes at most r points, where r is the number of orbits under the action of $\rho(P)$ (including the fixed point of part (a)).
132. Let G be a finite group acting faithfully and transitively on a set Ω . Assume that there exists a normal subgroup N such that N acts regularly on Ω (i.e., $G = G_\alpha N$ and $G_\alpha \cap N = 1$ for all $\alpha \in \Omega$). Prove that G_α embeds as a subgroup of $\text{Aut}(N)$.

Sylow Theorems

133. (a) Let G be a finite p -group acting on the finite set S . Let S_0 be the set of all elements of S fixed by G . Show that $|S| \equiv |S_0| \pmod{p}$.
- (b) Show that if H is a p -subgroup of a finite group G , then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.
- (c) State and prove Sylow's theorems.
134. Let G be a finite group and let P be a Sylow p -subgroup of G . Prove the following.
- (a) If M is any normal p -subgroup of G then $M \leq P$.
- (b) There is a normal p -subgroup N of G that contains all normal p -subgroups of G .
135. Let n be an integer and p a prime dividing n . Assume that there exists exactly one divisor d of n satisfying both $d > 1$ and $d \equiv 1 \pmod{p}$. Prove that if G is any finite group of order n and P is a Sylow p -subgroup of G , then either $P \trianglelefteq G$ or else $N_G(P)$ is a maximal subgroup of G .
136. Let G be a group of order 168 and let P be a Sylow 7-subgroup of G . Show that either P is a normal subgroup of G or else the normalizer of P is a maximal subgroup of G .
137. Show that if G is a simple group of order 60 then $G \cong A_5$.

138. Show that a group of order $2001 = 3 \cdot 23 \cdot 29$ contains a normal cyclic subgroup of index 3.
139. Show that if G is a group of order $2002 = 2 \cdot 7 \cdot 11 \cdot 13$, then G has an abelian subgroup of index 2.
140. Show that a group of order $2004 = 2^2 \cdot 3 \cdot 167$ must be solvable. Give an example of a group of order 2004 in which a Sylow 3-subgroup is not a normal subgroup.
141. Show that if G is a group of order $2010 = 2 \cdot 3 \cdot 5 \cdot 67$, then G has a normal subgroup of order 5.
142. Prove that a group G of order 36 must have a normal subgroup of order 3 or 9.
143. Show that a group of order 96 must have a normal subgroup of order 16 or 32.
144. Show that a group of order $160 = 2^5 \cdot 5$ must contain a nontrivial normal 2-subgroup.
145. Show that if G is a group of order $392 = 2^3 \cdot 7^2$, then G has a normal subgroup of order 7 or a normal subgroup of order 49.
146. Let G be a finite simple group containing an element of order 9. Show that every proper subgroup of G has index at least 9.
147. Show that there is no simple group of order 120.
148. (a) Show that S_6 has no simple subgroup of index 4 (i.e. order 180).
 (b) Show that a group of order $180 = 2^2 \cdot 3^2 \cdot 5$ cannot be simple.
149. (a) Show that $|\text{Aut}(\mathbb{Z}_7)| = 6$.
 (b) Show that a group of order 63 must contain an element of order 21.
150. Show that a simple group of order 168 must be isomorphic to a subgroup of the alternating group A_8 .
151. Let G be a simple group of order 168. Determine the number of elements of G of order 7. Explain your answer.
152. Let $p > q$ be primes. Show that if $p - 1$ is not divisible by q , then there is exactly one group of order pq .
153. Let G be a group of order pqr , where $p > q > r$ are primes. Let P be a Sylow p -subgroup of G and assume P is not normal in G . Show that a Sylow q -subgroup of G must be normal.
154. Let G be a group of order pqr , where $p > q > r$ are primes. Show that if $p - 1$ is not divisible by q , then a Sylow p -subgroup of G must be normal.
155. Let G be a group of order pqr , where $p > q > r$ are primes. Show that if $p - 1$ is not divisible by q or r and $q - 1$ is not divisible by r , then G must be abelian (hence cyclic).
 [Hint: Show that G' must be contained in a Sylow subgroup for two different primes.]
156. Let G be a group of order $105 = 3 \cdot 5 \cdot 7$. Prove that a Sylow 7-subgroup of G is normal.
157. Show that a group G of order $255 = 3 \cdot 5 \cdot 17$ must be abelian.

158. Let G be a group of order $231 = 3 \cdot 7 \cdot 11$. Prove that a Sylow 11-subgroup is contained in the center of G .
159. Show that a group of order $10000 = 2^4 \cdot 5^4$ cannot be simple.
160. Show that a group of order $3^3 \cdot 5 \cdot 13$ must have a normal Sylow 13-subgroup or a normal Sylow 5-subgroup. [Hint: Show that if a Sylow 13-subgroup is not normal, then a Sylow 13-subgroup must normalize a Sylow 5-subgroup. Consider the normalizer of a Sylow 5-subgroup.]
161. Let G be a group of order $3 \cdot 5 \cdot 7 \cdot 13$. Prove that G is not a simple group. [Hint: If a Sylow 7-subgroup is not normal, then some Sylow 13-subgroup will centralize it. Now compute the number of Sylow 13-subgroups.]
162. Let G be a group of order $p^n q$, where p and q are distinct primes, and assume $q \nmid p^i - 1$ for $1 \leq i \leq n - 1$. Prove that G is solvable.
163. Let p and q be distinct primes. Show that a group of order $p^2 q$ has a normal Sylow p -subgroup or a normal Sylow q -subgroup.
164. Let G be a group of order $(p + 1)p(p - 1)$ where p is a prime. Prove that the number of Sylow p -subgroups is either 1 or $p + 1$.
165. Show that a group of order $2^3 \cdot 3 \cdot 7^2$ is not simple.
166. Show that a group of order $380 = 2^2 \cdot 5 \cdot 19$ must be solvable.
167. Show that a group of order $2 \cdot 7 \cdot 13$ must be solvable.
168. Show that a group of order $1960 = 2^3 \cdot 5 \cdot 7^2$ must be solvable.
169. Prove that a group of order $1995 = 3 \cdot 5 \cdot 7 \cdot 19$ must be solvable.
170. Show that a group of order $1998 = 2 \cdot 3^3 \cdot 37$ must be solvable.
171. Let G be a group with exactly 31 Sylow 3-subgroups. Prove that there exist Sylow 3-subgroups P and Q satisfying $[P : P \cap Q] = [Q : P \cap Q] = 3$.
172. Let G be a finite group, p a prime divisor of $|G|$ and assume there are k distinct Sylow p -subgroups of G . Let $f : G \rightarrow S_k$ be the homomorphism of G into the symmetric group induced by the natural action of G by conjugation on the set of Sylow p -subgroups of G , and let $\overline{G} = f(G)$. Prove that \overline{G} has k distinct Sylow p -subgroups.
173. (a) Show that if K is a subgroup of G then the number of distinct conjugates of K in G is $[G : N_G(K)]$.
- (b) Show that if G has n_p Sylow p -subgroups, then G has a subgroup of index n_p .
174. Let G be a finite group and p a prime. Show that the intersection of all Sylow p -subgroups of G is a normal subgroup of G .
175. Let K be a normal subgroup of G and let P be a Sylow p -subgroup of K . Show that if $P \trianglelefteq K$ then $P \trianglelefteq G$.
176. Let G be a finite group and let P be a *normal* Sylow p -subgroup of G . Show that P is a characteristic subgroup of G .

177. A subgroup H of a group G is subnormal if there exists a chain $H = H_0 \leq H_1 \leq \cdots \leq H_k = G$ such that H_i is a normal subgroup of H_{i+1} for every i . Prove that if P is a Sylow p -subgroup of a finite group G then P is a subnormal in G if and only if P is normal in G .
178. Let G be a finite group and p a prime. Let N be a normal subgroup of G and H a Sylow p -subgroup of G . Show that
- HN/N is a Sylow p -subgroup of G/N , and
 - $H \cap N$ is a Sylow p -subgroup of N .
179. Let G be a finite group with subgroups H, K such that $G = HK$. Show that if p is any prime number, then there exist $P \in \text{Syl}_p(H)$ and $Q \in \text{Syl}_p(K)$ such that $PQ \in \text{Syl}_p(G)$.
180. Let G be a finite group, p a prime, and P a Sylow p -subgroup of G . Let H be a subgroup of G that contains the normalizer $N_G(P)$ of P in G . Show that if g is an element of G such that $g^{-1}Pg \leq H$, then g is an element of H .
181. Let G be a finite group, H be a subgroup of G , and P be a Sylow p -subgroup of H for some prime p . Show that if H contains the normalizer $N_G(P)$ of P , then P is a Sylow p -subgroup of G .
182. A subgroup H of a group G is called *pronormal* if, for any $g \in G$, H is conjugate to H^g in $\langle H, H^g \rangle$.
- Show that if $H \leq N \trianglelefteq G$ with H pronormal in G , then $G = N_G(H)N$.
 - Show that if P is a Sylow p -subgroup of G , then P is pronormal in G .
183. Let G be a finite group and H a normal subgroup. Show that if P is a Sylow p -subgroup of H , then $G = HN_G(P)$.
184. Let P be a Sylow p -subgroup of a group G and let K be a subgroup of G containing $N_G(P)$. Show that $N_G(K) = K$.
185. Let x and y be two elements of $Z(P)$ where P is a Sylow p -subgroup of G . If x and y are conjugate in G , prove that x is conjugate to y in $N_G(P)$.
186. (a) Let p be a prime and let H be a p -subgroup of the finite group G . Show that
- $$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$
- (Hint: Let H act on G/H by left multiplication.)
- Let P be a p -subgroup of G . Show that P is a Sylow p -subgroup of G if and only if P is a Sylow p -subgroup of $N_G(P)$.
187. Let G be a finite group with $|G| = p^a m$, where p is a prime and $p \nmid m$. Assume that whenever P and Q are Sylow p -subgroups of G , either $P = Q$ or $P \cap Q = 1$. Show that the number of Sylow p -subgroups of G is congruent to 1 modulo p^a .
188. Let P be a Sylow p -subgroup of the finite group G , and assume $|P| = p^a$. Suppose that $P \cap P^g = \{1\}$ whenever $g \in G$ does not normalize P . Prove that the number of Sylow p -subgroups of G is congruent to 1 mod p^a .

189. Let p be a prime and let P be a p -subgroup of the finite group G . Show that P is a Sylow p -subgroup of G if and only if P is a Sylow p -subgroup of $PC_G(P)$ and $[N_G(P) : PC_G(P)]$ is not divisible by p .
190. Let G be a finite group, and p a prime. Let n_p be the number of Sylow p -subgroups of G and suppose that p^e does *not* divide $n_p - 1$. Prove that there exist two distinct Sylow p -subgroups of G , say P and Q , satisfying $[P : P \cap Q] \leq p^e$.
191. Let P and Q be distinct Sylow p -subgroups of a finite group G . Prove that the number of Sylow p -subgroups of G is strictly greater than $[P : P \cap Q]$.
192. Let X and G be finite groups. We say that X is *involved* in G if there exist subgroups K and H of G , with K normal in H , such that X is isomorphic to H/K . Suppose X is a p -group, P is a Sylow p -subgroup of G , and X is involved in G . Prove that X is involved in P .

Solvable and Nilpotent Groups, Commutator and Frattini Subgroups

193. Show that the following statements are equivalent.
- (i) Every finite group of odd order is solvable.
 - (ii) Every non-abelian finite simple group is of even order.
194. Let H and K be subgroups of a group G with $K \trianglelefteq G$. Show that if H and K are solvable, then HK is solvable.
195. Let G be a solvable group and N a nontrivial normal subgroup of G . Show that there is a nontrivial abelian subgroup A of N with A normal in G .
196. Let G be a finite non-solvable group, each of whose proper subgroups is solvable. Show that $G/\Phi(G)$ is a non-abelian simple group, where $\Phi(G)$ denotes the Frattini subgroup of G .
197. We say that a group X is *involved* in a group G if X is isomorphic to H/K for some subgroups K, H of G with $K \trianglelefteq H$. Prove that if X is solvable and X is involved in the finite group G , then X is involved in a solvable subgroup of G .
198. Let G be a finite group satisfying the following property:
 (*) If A, B are subgroups of G then AB is a subgroup of G .
 Prove that G is a solvable group.
199. Let X be a set of operators for the group G and assume that G is a finite solvable group. Prove that every X -composition factor in any X -composition series for G is an elementary abelian p -group for some prime p .
200. Show that if G is a nilpotent group and $\langle 1 \rangle \neq N \trianglelefteq G$, then $N \cap Z(G) \neq \langle 1 \rangle$.
201. Show that if G is a nilpotent finite group, then every subgroup of prime index is a normal subgroup.

202. (a) Show that if G is a group and H, K are subgroups of G such that $HK \subseteq KH$, then HK is a subgroup of G .
- (b) Suppose G is finite and $HK \subseteq KH$ for all subgroups H and K of G . Show that if p is a prime divisor of $|G|$, then there is a subgroup N of G such that $|G : N|$ is a power of p and $p \nmid |N|$.
203. Let G be a finite group and let $\Phi(G)$ be its Frattini subgroup. Show that $\Phi(G)$ is precisely the set of non-generators of G . (An element g of G is called a non-generator if for any subset S of G containing g and generating G , the set $S - \{g\}$ also generates G .)
204. Let $\langle 1 \rangle = G_0 \leq G_1 \leq \dots \leq G_n = G$ be a central series for the nilpotent group G . Prove that $G_i \leq Z_i(G)$ for all i , where $\{Z_i(G)\}$ is the upper central series of G . Thus, among all central series for a nilpotent group, the upper central series ascends the fastest.
205. Let G be a finite group, let $\Phi(G)$ be the Frattini subgroup of G (that is, the intersection of all maximal subgroups of G) and let G' be the commutator subgroup of G . Show that the following are equivalent.
- The group G is nilpotent.
 - If H is a proper subgroup of G , then H is a proper subgroup of its normalizer in G .
 - Every maximal subgroup of G is a normal subgroup of G .
 - $G' \leq \Phi(G)$.
 - Every Sylow subgroup of G is a normal subgroup of G .
 - The group G is a direct product of its Sylow subgroups.
206. Let G be a finite group. Show that each of the following conditions is equivalent to the nilpotence of G .
- Whenever $x, y \in G$ satisfy $(|x|, |y|) = 1$, then $xy = yx$.
 - Whenever p and q are distinct primes and $P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_q(G)$, then P centralizes Q .
207. Show that if G is a finite nilpotent group and m is a positive integer such that m divides the order of G , then G has a subgroup of order m .
208. Let G be a finite nilpotent group and G' its commutator subgroup. Show that if G/G' is cyclic then G is cyclic.
209. A finite group G is called an N -group if the normalizer $N_G(P)$ of every non-identity p -subgroup P of G is solvable. Prove that if G is an N -group, then either (i) G is solvable, or (ii) G has a unique minimal normal subgroup K , the factor group G/K is solvable, and K is simple.
210. Let G be a finite group and let N be a normal subgroup of G with the property that G/N is nilpotent. Prove that there exists a nilpotent subgroup H of G satisfying $G = HN$.
211. Let G be a finite solvable group. Prove that the index of every maximal subgroup is a prime power.
212. **[NEW]**
Let G be a group. Show that if $g \in G$, then the conjugacy class of g is contained in gG' .

213. Let G be a group of odd order. Let g_1, \dots, g_n be the elements of G , listed in any order.

Show that $\prod_{i=1}^n g_i$ is an element of the commutator subgroup G' of G .

214. Let G be a finite group and let M be a maximal subgroup of G .

(a) Show that if $Z(G)$ is not contained in M , then $M \trianglelefteq G$.

(b) Show that either $Z(G) \leq M$ or $G' \leq M$.

(c) Show that $Z(G) \cap G' \leq \Phi(G)$.

RING THEORY

General Ring Theory

1. Give an example of each of the following.
 - (a) An irreducible polynomial of degree 3 in $\mathbf{Z}_3[x]$.
 - (b) A polynomial in $\mathbb{Z}[x]$ that is not irreducible in $\mathbb{Z}[x]$ but is irreducible in $\mathbb{Q}[x]$.
 - (c) A non-commutative ring of characteristic p , p a prime.
 - (d) A ring with exactly 6 invertible elements.
 - (e) An infinite non-commutative ring with only finitely many ideals.
 - (f) An infinite non-commutative ring with non-zero characteristic.
 - (g) An integral domain which is not a unique factorization domain.
 - (h) A unique factorization domain that is not a principal ideal domain.
 - (i) A principal ideal domain that is not a Euclidean domain.
 - (j) A Euclidean domain other than the ring of integers or a field.
 - (k) A finite non-commutative ring.
 - (l) A commutative ring with a sequence $\{P_n\}_{n=1}^{\infty}$ of prime ideals such that P_n is properly contained in P_{n+1} for all n .
 - (m) A non-zero prime ideal of a commutative ring that is not a maximal ideal.
 - (n) An irreducible element of a commutative ring that is not a prime element.
 - (o) An irreducible element of an integral domain that is not a prime element.
 - (p) A commutative ring that has exactly one maximal ideal and is not a field.
 - (q) A non-commutative ring with exactly two maximal ideals.
2.
 - (a) How many units does the ring $\mathbb{Z}/60\mathbb{Z}$ have? Explain your answer.
 - (b) How many ideals does the ring $\mathbb{Z}/60\mathbb{Z}$ have? Explain your answer.
3. Denote the set of invertible elements of the ring \mathbb{Z}_n by U_n .
 - (a) List all the elements of U_{18} .
 - (b) Is U_{18} a cyclic group under multiplication? Justify your answer.
4. If p is a prime satisfying $p \equiv 1 \pmod{4}$, then p is a sum of two squares.
5. If (\cdot) denotes the Legendre symbol, prove Euler's Criterion: if p is a prime and a is any integer relatively prime to p , then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.
6. Let R_1 and R_2 be commutative rings with identities and let $R = R_1 \times R_2$. Show that every ideal I of R is of the form $I = I_1 \times I_2$ with I_i an ideal of R_i for $i = 1, 2$.
7. Show that a non-zero ring R in which $x^2 = x$ for all $x \in R$ is of characteristic 2 and is commutative.
8. Let R be a finite commutative ring with more than one element and no zero-divisors. Show that R is a field.

9. Determine for which integers n the ring $\mathbb{Z}/n\mathbb{Z}$ is a direct sum of fields. Prove your answer.
10. Let R be a subring of a field F such that for each x in F either $x \in R$ or $x^{-1} \in R$. Prove that if I and J are two ideals of R , then either $I \subseteq J$ or $J \subseteq I$.
11. The *Jacobson Radical* $J(R)$ of a ring R is defined to be the intersection of all maximal ideals of R .
Let R be a commutative ring with 1 and let $x \in R$. Show that $x \in J(R)$ if and only if $1 - xy$ is a unit for all y in R .
12. Let R be any ring with identity, and n any positive integer. If $M_n(R)$ denotes the ring of $n \times n$ matrices with entries in R , prove that $M_n(I)$ is an ideal of $M_n(R)$ whenever I is an ideal of R , and that every ideal of $M_n(R)$ has this form.
13. Let m, n be positive integers such that m divides n . Then the natural map $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ given by $a + (n) \mapsto a + (m)$ is a surjective ring homomorphism. If U_n, U_m are the units of \mathbb{Z}_n and \mathbb{Z}_m , respectively, show that $\varphi : U_n \rightarrow U_m$ is a surjective group homomorphism.
14. Let R be a ring with ideals A and B . Let $R/A \times R/B$ be the ring with coordinate-wise addition and multiplication. Show the following.
(a) The map $R \rightarrow R/A \times R/B$ given by $r \mapsto (r + A, r + B)$ is a ring homomorphism.
(b) The homomorphism in part (a) is surjective if and only if $A + B = R$.
15. Let m and n be relatively prime integers.
(a) Show that if c and d are any integers, then there is an integer x such that $x \equiv c \pmod{m}$ and $x \equiv d \pmod{n}$.
(b) Show that \mathbb{Z}_{mn} and $\mathbb{Z}_m \times \mathbb{Z}_n$ are isomorphic as rings.
16. Let R be a commutative ring with 1 and let I and J be ideals of R such that $I + J = R$. Show that $R/(I \cap J) \cong R/I \oplus R/J$.
17. Let R be a commutative ring, not necessarily with identity, and assume there is some fixed positive integer n such that $nr = 0$ for all $r \in R$. Prove that R embeds in a ring S with identity so that R is an ideal of S and $S/R \cong \mathbb{Z}/n\mathbb{Z}$.
18. Let R be a ring with identity 1 and $a, b \in R$ such that $ab = 1$. Denote $X = \{x \in R \mid ax = 1\}$. Show the following.
(a) If $x \in X$, then $b + (1 - xa) \in X$.
(b) If $\varphi : X \rightarrow X$ is the mapping given by $\varphi(x) = b + (1 - xa)$, then φ is one-to-one.
(c) If X has more than one element, then X is an infinite set.
19. Let R be a commutative ring with identity and define $U_2(R) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in R \right\}$.
Prove that every R -automorphism of $U_2(R)$ is inner.
20. Let \mathbb{R} be the field of real numbers and let F be the set of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}$, where $a, b \in \mathbb{R}$. Show that F is a field under the usual matrix operations.
21. Let R be the ring of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ where a and b are real numbers.
Prove that R is isomorphic to \mathbb{C} , the field of complex numbers.

22. Let p be a prime and let R be the ring of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ pb & a \end{bmatrix}$, where $a, b \in \mathbb{Z}$. Prove that R is isomorphic to $\mathbb{Z}[\sqrt{p}]$.
23. Let p be a prime and F_p the set of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where $a, b \in \mathbb{Z}_p$.
- Show that F_p is a commutative ring with identity.
 - Show that F_7 is a field.
 - Show that F_{13} is not a field.
24. Let $I \subseteq J$ be right ideals of a ring R such that $J/I \cong R$ as right R -modules. Prove that there exists a right ideal K such that $I \cap K = (0)$ and $I + K = J$.
25. A ring R is called simple if $R^2 \neq 0$ and 0 and R are its only ideals. Show that the center of a simple ring is 0 or a field.
26. Give an example of a field F and a one-to-one ring homomorphism $\varphi : F \rightarrow F$ which is not onto. Verify your example.
27. Let D be an integral domain and let $D[x_1, x_2, \dots, x_n]$ be the polynomial ring over D in the n indeterminates x_1, x_2, \dots, x_n . Let

$$V = \begin{bmatrix} x_1^{n-1} & \cdots & x_1^2 & x_1 & 1 \\ x_2^{n-1} & \cdots & x_2^2 & x_2 & 1 \\ \vdots & & \vdots & \vdots & \vdots \\ x_n^{n-1} & \cdots & x_n^2 & x_n & 1 \end{bmatrix}.$$

Prove that the determinant of V is $\prod_{1 \leq i < j \leq n} (x_i - x_j)$.

28. Let $R = C[0, 1]$ be the set of all continuous real-valued functions on $[0, 1]$. Define addition and multiplication on R as follows. For $f, g \in R$ and $x \in [0, 1]$,
- $$(f + g)(x) = f(x) + g(x) \text{ and } (fg)(x) = f(x)g(x).$$
- Show that R with these operations is a commutative ring with identity.
 - Find the units of R .
 - If $f \in R$ and $f^2 = f$, then $f = 0_R$ or $f = 1_R$.
 - If n is a positive integer and $f \in R$ is such that $f^n = 0_R$, then $f = 0_R$.
29. Let S be the ring of all bounded, continuous functions $f : \mathbb{R} \rightarrow \mathbb{R}$, where \mathbb{R} is the set of real numbers. Let I be the set of functions f in S such that $f(t) \rightarrow 0$ as $|t| \rightarrow \infty$.
- Show that I is an ideal of S .
 - Suppose $x \in S$ is such that there is an $i \in I$ with $ix = x$. Show that $x(t) = 0$ for all sufficiently large $|t|$.
30. Let \mathbb{Q} be the field of rational numbers and $D = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
- Show that D is a subring of the field of real numbers.
 - Show that D is a principal ideal domain.
 - Show that $\sqrt{3}$ is not an element of D .

31. Show that if p is a prime such that $p \equiv 1 \pmod{4}$, then $x^2 + 1$ is not irreducible in $\mathbb{Z}_p[x]$.
32. Show that if p is a prime such that $p \equiv 3 \pmod{4}$, then $x^2 + 1$ is irreducible in $\mathbb{Z}_p[x]$.
33. Show that if p is a prime such that $p \equiv 1 \pmod{6}$, then $x^3 + 1$ splits in $\mathbb{Z}_p[x]$.

Prime, Maximal, and Primary Ideals

34. Let R be a non-zero commutative ring with 1. Show that an ideal M of R is maximal if and only if R/M is a field.
35. (a) Let R be a commutative ring with 1. Show that if M is a maximal ideal of R then M is a prime ideal of R .
(b) Give an example of a non-zero prime ideal in a ring R that is not a maximal ideal.
36. Let R be a non-zero ring with identity. Show that every proper ideal of R is contained in a maximal ideal.
37. Let R be a non-zero commutative ring with 1. Show that if I is an ideal of R such that $1 + a$ is a unit in R for all $a \in I$, then I is contained in every maximal ideal of R .
38. Let R be a commutative ring with 1.
(a) Prove that (x) is a prime ideal in $R[x]$ if and only if R is an integral domain.
(b) Prove that (x) is a maximal ideal in $R[x]$ if and only if R is a field.
39. Find all values of a in \mathbb{Z}_3 such that the quotient ring

$$\mathbb{Z}_3[x]/(x^3 + x^2 + ax + 1)$$

is a field. Justify your answer.

40. Find all values of a in \mathbb{Z}_5 such that the quotient ring

$$\mathbb{Z}_5[x]/(x^3 + 2x^2 + ax + 3)$$

is a field. Justify your answer.

41. Let R be a commutative ring with identity and let U be maximal among non-finitely generated ideals of R . Prove U is a prime ideal.
42. Let R be a commutative ring with identity and let U be maximal among non-principal ideals of R . Prove U is a prime ideal.
43. Let R be a non-zero commutative ring with 1 and S a multiplicative subset of R not containing 0. Show that if P is maximal in the set of ideals of R not intersecting S , then P is a prime ideal.
44. Let R be a non-zero commutative ring with 1.
(a) Let S be a multiplicative subset of R not containing 0 and let P be maximal in the set of ideals of R not intersecting S . Show that P is a prime ideal.
(b) Show that the set of nilpotent elements of R is the intersection of all prime ideals.

45. Let R be a commutative ring with identity and let S be the set of all elements of R that are *not* zero-divisors. Show that there is a prime ideal P such that $P \cap S$ is empty. (Hint: Use Zorn's Lemma.)
46. Let R be a commutative ring with identity and let \mathcal{C} be a chain of prime ideals of R . Show that $\bigcup_{P \in \mathcal{C}} P$ and $\bigcap_{P \in \mathcal{C}} P$ are prime ideals of R .
47. Let R be a commutative ring and P a prime ideal of R . Show that there is a prime ideal $P_0 \subseteq P$ which does not properly contain any prime ideal.
48. Let R be a commutative ring with 1 such that for every x in R there is an integer $n > 1$ (depending on x) such that $x^n = x$. Show that every prime ideal of R is maximal.
49. Let R be a commutative ring with 1 in which every ideal is a prime ideal. Prove that R is a field. (Hint: For $a \neq 0$ consider the ideals (a) and (a^2) .)
50. Let D be a principal ideal domain. Prove that every nonzero prime ideal of D is a maximal ideal.
51. Show that if R is a finite commutative ring with identity then every prime ideal of R is a maximal ideal.
52. Let $R = C[0, 1]$ be the ring of all continuous real-valued functions on $[0, 1]$, with addition and multiplication defined as follows. For $f, g \in R$ and $x \in [0, 1]$,
- $$(f + g)(x) = f(x) + g(x)$$
- $$(fg)(x) = f(x)g(x).$$
- Prove that if M is a maximal ideal of R , then there is a real number $x_0 \in [0, 1]$ such that $M = \{f \in R \mid f(x_0) = 0\}$.
53. Let R be a commutative ring with identity, and let $P \subset Q$ be prime ideals of R . Prove that there exist prime ideals P^*, Q^* satisfying $P \subseteq P^* \subset Q^* \subseteq Q$, such that there are no prime ideals strictly between P^* and Q^* . HINT: Fix $x \in Q - P$ and show that there exists a prime ideal P^* containing P , contained in Q and maximal with respect to not containing x .
54. Let R be a commutative ring with 1. An ideal I of R is called a *primary* ideal if $I \neq R$ and for all $x, y \in R$ with $xy \in I$, either $x \in I$ or $y^n \in I$ for some integer $n \geq 1$.
- (a) Show that an ideal I of R is primary if and only if $R/I \neq 0$ and every zero-divisor in R/I is nilpotent.
- (b) Show that if I is a primary ideal of R then the radical $\text{Rad}(I)$ of I is a prime ideal. (Recall that $\text{Rad}(I) = \{x \in R \mid x^n \in I \text{ for some } n\}$.)

Commutative Rings

55. Let R be a commutative ring with identity. Show that R is an integral domain if and only if R is a subring of a field.
56. Let R be a commutative ring with identity. Show that if x and y are nilpotent elements of R then $x + y$ is nilpotent and the set of all nilpotent elements is an ideal in R .

57. Let R be a commutative ring with identity. An ideal I of R is *irreducible* if it cannot be expressed as the intersection of two ideals of R neither of which is contained in the other. Show the following.
- If P is a prime ideal then P is irreducible.
 - If x is a non-zero element of R , then there is an ideal I_x , maximal with respect to the property that $x \notin I_x$, and I_x is irreducible.
 - If every irreducible ideal of R is a prime ideal, then 0 is the only nilpotent element of R .
58. Let R be a commutative ring with 1 and let I be an ideal of R satisfying $I^2 = \{0\}$. Show that if $a + I \in R/I$ is an idempotent element of R/I , then the coset $a + I$ contains an idempotent element of R .
59. Let R be a commutative ring with identity that has exactly one prime ideal P . Prove the following.
- R/P is a field.
 - R is isomorphic to R_P , the ring of quotients of R with respect to the multiplicative set $R - P = \{s \in R \mid s \notin P\}$.
60. Let R be a commutative ring with identity and $\sigma : R \rightarrow R$ a ring automorphism.
- Show that $F = \{r \in R \mid \sigma(r) = r\}$ is a subring of R and the identity of R is in F .
 - Show that if σ^2 is the identity map on R , then each element of R is the root of a monic polynomial of degree two in $F[x]$.
61. Let R be a commutative ring with identity that has exactly three ideals, $\{0\}$, I , and R .
- Show that if $a \notin I$, then a is a unit of R .
 - Show that if $a, b \in I$ then $ab = 0$.
62. Let R be a commutative ring with 1. Show that if u is a unit in R and n is nilpotent, then $u + n$ is a unit.
63. Let R be a commutative ring with identity. Suppose that for every $a \in R$, either a or $1 - a$ is invertible. Prove that $N = \{a \in R \mid a \text{ is not invertible}\}$ is an ideal of R .
64. Let R be a commutative ring with 1. Show that the sum of any two principal ideals of R is principal if and only if every finitely generated ideal of R is principal.
65. Let R be a commutative ring with identity such that not every ideal is a principal ideal.
- Show that there is an ideal I maximal with respect to the property that I is not a principal ideal.
 - If I is the ideal of part (a), show that R/I is a principal ideal ring.
66. Recall that if $R \subseteq S$ is an inclusion of commutative rings (with the same identity) then an element $s \in S$ is *integral over R* if s satisfies some monic polynomial with coefficients in R . Prove the equivalence of the following statements.
- s is integral over R .
 - $R[s]$ is finitely generated as an R -module.
 - There exists a faithful $R[s]$ module which is finitely generated as an R -module.

67. Recall that if $R \subseteq S$ is an inclusion of commutative rings (with the same identity) then S is an *integral* extension of R if every element of S satisfies some monic polynomial with coefficients in R . Prove that if $R \subseteq S \subseteq T$ are commutative rings with the same identity, then S is integral over R and T is integral over S if and only if T is integral over R .
68. Let $R \subseteq S$ be commutative domains with the same identity, and assume that S is an integral extension of R . Let I be a nonzero ideal of S . Prove that $I \cap R$ is a nonzero ideal of R .

Domains

69. Suppose R is a domain and I and J are ideals of R such that IJ is principal. Show that I (and hence J) is finitely generated.
 [Hint: If $IJ = (a)$, then $a = \sum_{i=1}^n x_i y_i$ for some $x_i \in I$ and $y_i \in J$. Show the x_i generate I .]
70. Show that if p is a prime such that there is an integer b with $p = b^2 + 4$, then $\mathbb{Z}[\sqrt{p}]$ is not a unique factorization domain.
71. Show that if p is a prime such that $p \equiv 1 \pmod{4}$, then $\mathbb{Z}[\sqrt{p}]$ is not a unique factorization domain.
72. Let $D = \mathbb{Z}(\sqrt{5}) = \{m + n\sqrt{5} \mid m, n \in \mathbb{Z}\}$ — a subring of the field of real numbers and necessarily an integral domain (you need not show this) — and $F = \mathbb{Q}(\sqrt{5})$ its field of fractions. Show the following:
 (a) $x^2 + x - 1$ is irreducible in $D[x]$ but not in $F[x]$.
 (b) D is not a unique factorization domain.
73. Let $D = \mathbb{Z}(\sqrt{21}) = \{m + n\sqrt{21} \mid m, n \in \mathbb{Z}\}$ and $F = \mathbb{Q}(\sqrt{21})$, the field of fractions of D . Show the following:
 (a) $x^2 - x - 5$ is irreducible in $D[x]$ but not in $F[x]$.
 (b) D is not a unique factorization domain.
74. Let $D = \mathbb{Z}(\sqrt{-11}) = \{m + n\sqrt{-11} \mid m, n \in \mathbb{Z}\}$ and $F = \mathbb{Q}(\sqrt{-11})$ its field of fractions. Show the following:
 (a) $x^2 - x + 3$ is irreducible in $D[x]$ but not in $F[x]$.
 (b) D is not a unique factorization domain.
75. **[NEW]**
 Let $D = \mathbb{Z}(\sqrt{13}) = \{m + n\sqrt{13} \mid m, n \in \mathbb{Z}\}$ and $F = \mathbb{Q}(\sqrt{13})$ its field of fractions. Show the following:
 (a) $x^2 + 3x - 1$ is irreducible in $D[x]$ but not in $F[x]$.
 (b) D is not a unique factorization domain.
76. Let D be an integral domain and F a subring of D which is a field. Show that if each element of D is algebraic over F , then D is a field.
77. Let D be an integral domain.
 (a) For $a, b \in D$ define a *greatest common divisor* of a and b .
 (b) For $x \in D$ denote $(x) = \{dx \mid d \in D\}$. Prove that if $(a) + (b) = (d)$, then d is a greatest common divisor of a and b .

78. Let D be a principal ideal domain.
- For $a, b \in D$, define a *least common multiple* of a and b .
 - Show that $d \in D$ is a least common multiple of a and b if and only if $(a) \cap (b) = (d)$.
79. Let D be a principal ideal domain and let $a, b \in D$.
- Show that there is an element $d \in D$ that satisfies the properties
 - $d|a$ and $d|b$ and
 - if $e|a$ and $e|b$ then $e|d$.
 - Show that there is an element $m \in D$ that satisfies the properties
 - $a|m$ and $b|m$ and
 - if $a|e$ and $b|e$ then $m|e$.
80. Let R be a principal ideal domain. Show that if (a) is a nonzero ideal in R , then there are only finitely many ideals in R containing (a) .
81. Let D be a unique factorization domain and F its field of fractions. Prove that if d is an irreducible element in D , then there is no $x \in F$ such that $x^2 = d$.
82. Let D be a Euclidean domain. Prove that every non-zero prime ideal is a maximal ideal.
83. Let D with $\varphi : D - \{0\} \rightarrow \mathbb{N}$ be a Euclidean domain. Suppose $\varphi(a + b) \leq \max\{\varphi(a), \varphi(b)\}$ for all $a, b \in D$. Prove that D is either a field or isomorphic to a polynomial ring over a field.
84. Let D be an integral domain and F its field of fractions. Show that if g is an isomorphism of D onto itself, then there is a unique isomorphism h of F onto F such that $h(d) = g(d)$ for all d in D .
85. Let D be a unique factorization domain such that if p and q are irreducible elements of D , then p and q are associates. Show that if A and B are ideals of D , then either $A \subseteq B$ or $B \subseteq A$.
86. Let D be a unique factorization domain and p a fixed irreducible element of D such that if q is any irreducible element of D , then q is an associate of p . Show the following.
- If d is a nonzero element of D , then d is uniquely expressible in the form up^n , where u is a unit of D and n is a non-negative integer.
 - D is a Euclidean domain.
87. Prove that $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain.
88. Show that the ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean ring and compute the greatest common divisor of $5 + i$ and 13 using the Euclidean algorithm.

Polynomial Rings

89. Show that the polynomial $f(x) = x^4 + 5x^2 + 3x + 2$ is irreducible over the field of rational numbers.
90. Let D be an integral domain and $D[x]$ the polynomial ring over D . Suppose $\varphi : D[x] \rightarrow D[x]$ is an isomorphism such that $\varphi(d) = d$ for all $d \in D$. Show that $\varphi(x) = ax + b$ for some $a, b \in D$ and that a is a unit of D .

91. Let $f(x) = a_0 + a_1x + \cdots + a_kx^k + \cdots + a_nx^n \in \mathbb{Z}[x]$ and p a prime such that $p|a_i$ for $i = 1, \dots, k-1$, $p \nmid a_k$, $p \nmid a_n$, and $p^2 \nmid a_0$. Show that $f(x)$ has an irreducible factor in $\mathbb{Z}[x]$ of degree at least k .
92. Let D be an integral domain and $D[x]$ the polynomial ring over D in the indeterminate x . Show that if every nonzero prime ideal of $D[x]$ is a maximal ideal, then D is a field.
93. Let R be a commutative ring with 1 and let $f(x) \in R[x]$ be nilpotent. Show that the coefficients of f are nilpotent.
94. Show that if R is an integral domain and $f(x)$ is a unit in the polynomial ring $R[x]$, then $f(x)$ is in R .
95. Let D be a unique factorization domain and F its field of fractions. Prove that if $f(x)$ is a monic polynomial in $D[x]$ and $\alpha \in F$ is a root of f , then $\alpha \in D$.
96. (a) Show that $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_3[x]$.
 (b) Show that $x^4 + 1$ is not irreducible in $\mathbb{Z}_3[x]$.
97. Let $F[x, y]$ be the polynomial ring over a field F in two indeterminates x, y . Show that the ideal generated by $\{x, y\}$ is not a principal ideal.
98. Let D be an integral domain and let c be an irreducible element in D . Show that the ideal (x, c) generated by x and c in the polynomial ring $D[x]$ is not a principal ideal.
99. Show that if R is a commutative ring with 1 that is not a field, then $R[x]$ is not a principal ideal ring.
100. (a) Let $\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \mid a, n \in \mathbb{Z}, n \geq 0\}$, the smallest subring of \mathbb{Q} containing \mathbb{Z} and $\frac{1}{2}$. Let $(2x-1)$ be the ideal of $\mathbb{Z}[x]$ generated by the polynomial $2x-1$. Show that $\mathbb{Z}[x]/(2x-1) \cong \mathbb{Z}[\frac{1}{2}]$.
 (b) Find an ideal I of $\mathbb{Z}[x]$ such that $(2x-1) \subsetneq I \subsetneq \mathbb{Z}[x]$.

Non-commutative Rings

101. Let R be a ring with identity such that the identity map is the only ring automorphism of R . Prove that the set N of all nilpotent elements of R is an ideal of R .
102. Let p be a prime. A ring S is called a p -ring if the characteristic of S is a power of p . Show that if R is a ring with identity of finite characteristic, then R is isomorphic to a finite direct product of p -rings for distinct primes.
103. Let R be a ring.
- (a) Show that there is a unique smallest (with respect to inclusion) ideal A such that R/A is a commutative ring.
- (b) Give an example of a ring R such that for every proper ideal I , R/I is not commutative. Verify your example.
- (c) For the ring $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z} \right\}$ with the usual matrix operations, find the ideal A of part (a).

104. If R is any ring with identity, let $J(R)$ denote the Jacobson radical of R . If e is any idempotent of R , show that $J(eRe) = eJ(R)e$.
105. If n is a positive integer and F is any field, let $M_n(F)$ denote the ring of $n \times n$ matrices with entries in F . Prove that $M_n(F)$ is a simple ring. Equivalently, $\text{End}_F(V)$ is a simple ring if V is a finite dimensional vector space over F .
106. A ring R is *nilpotent-free* if $a^n = 0$ for $a \in R$ and some positive integer n implies $a = 0$.
- Suppose there is an ideal I such that R/I is nilpotent-free. Show there is a unique smallest (with respect to inclusion) ideal A such that R/A is nilpotent-free.
 - Give an example of a ring R such that for every proper ideal I , R/I is not nilpotent-free. Verify your example.
 - Show that if R is a commutative ring with identity, then there is a proper ideal I of R such that R/I is nilpotent-free, and find the ideal A of part (a).

Local Rings, Localization, Rings of Fractions

107. Let R be an integral domain. Construct the field of fractions F of R by defining the set F and the two binary operations, and show that the two operations are well-defined. Show that F has a multiplicative identity element and that every nonzero element of F has a multiplicative inverse.
108. A *local* ring is a commutative ring with 1 that has a unique maximal ideal. Show that a ring R is local if and only if the set of non-units in R is an ideal.
109. Let R be a commutative ring with $1 \neq 0$ in which the set of nonunits is closed under addition. Prove that R is local, i.e., has a unique maximal ideal.
110. Let D be an integral domain and F its field of fractions. Let P be a prime ideal in D and $D_P = \{ab^{-1} \mid a, b \in D, b \notin P\} \subseteq F$. Show that D_P has a unique maximal ideal.
111. Let R be a commutative ring with identity and M a maximal ideal of R . Let R_M be the ring of quotients of R with respect to the multiplicative set $R - M = \{s \in R \mid s \notin M\}$. Show the following.
- $M_M = \{\frac{a}{s} \mid a \in M, s \notin M\}$ is the unique maximal ideal of R_M .
 - The fields R/M and R_M/M_M are isomorphic.
112. Let R be an integral domain, S a multiplicative set, and let $S^{-1}R = \{\frac{r}{s} \mid r \in R, s \in S\}$ (contained in the field of fractions of R). Show that if P is a prime ideal of R then, $S^{-1}P$ is either a prime ideal of $S^{-1}R$ or else equals $S^{-1}R$.
113. Let R be a commutative ring with identity and P a prime ideal of R . Let R_P be the ring of quotients of R with respect to the set $R - P = \{s \in R \mid s \notin P\}$. Show that R_P/P_P is the field of fractions of the integral domain R/P .
114. Let D be an integral domain and F its field of fractions. Denote by \mathcal{M} the set of all maximal ideals of D . For $M \in \mathcal{M}$, let $D_M = \{\frac{a}{s} \mid a, s \in D, s \notin M\} \subset F$. Show that $\bigcap_{M \in \mathcal{M}} D_M = D$.

115. Let R be a commutative ring with 1 and D a multiplicative subset of R containing 1. Let J be an ideal in the ring of fractions $D^{-1}R$ and let

$$I = \{ a \in R \mid \frac{a}{d} \in J \text{ for some } d \in D \}.$$

Show that I is an ideal of R .

116. Let D be a principal ideal domain and let P be a non-zero prime ideal. Show that D_P , the localization of D at P , is a principal ideal domain and has a unique irreducible element, up to associates.

Chains and Chain Conditions

117. Let R be a commutative ring with identity. Prove that any non-empty set of prime ideals of R contains maximal *and* minimal elements.
118. Let R be a commutative ring with 1. We say R satisfies the *ascending chain condition* if whenever $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is an ascending chain of ideals, there is an integer N such that $I_k = I_N$ for all $k \geq N$. Show that R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.
119. Let R be a commutative Noetherian ring with identity. Prove that there are only finitely many *minimal* prime ideals of R .
120. Let R be a commutative Noetherian ring with identity and let I be an ideal in R . Let $J = \text{Rad}(I)$. Prove that there exists a positive integer n such that $j^n \in I$ for all $j \in J$.
121. Let R be a commutative Noetherian domain with identity. Prove that every nonzero ideal of R contains a product of nonzero *prime* ideals of R .
122. Let R be a ring satisfying the *descending chain condition* on right ideals. If $J(R)$ denotes the Jacobson radical of R , prove that $J(R)$ is nilpotent.
123. Show that if R is a commutative Noetherian ring with identity, then the polynomial ring $R[x]$ is also Noetherian.
124. Let P be a nonzero prime ideal of the commutative Noetherian domain R . Assume P is principal. Prove that there does not exist a prime ideal Q satisfying $(0) < Q < P$.
125. Let R be a commutative Noetherian ring. Prove that every nonzero ideal A of R contains a product of prime ideals (not necessarily distinct) each of which contains A .
126. Let R be a commutative ring with 1 and let M be an R -module that is not Artinian (Noetherian, of finite composition length). Let \mathcal{I} be the set of ideals I of R such that there exists an R -submodule N of M with the property that N/NI is not Artinian (Noetherian, of finite composition length, respectively). Show that if $A \in \mathcal{I}$ is a maximal element of \mathcal{I} , then A is a prime ideal of R .

FIELD THEORY

General Field Theory

1. Prove or disprove each of the following statements.
 - (a) If K is a subfield of F and F is isomorphic to K , then $F = K$.
 - (b) The field \mathbb{C} of complex numbers is an algebraic closure of the field \mathbb{Q} of rational numbers.
 - (c) If K is a finitely generated extension of F , then $[K : F]$ is finite.
 - (d) If K is a finitely generated algebraic extension of F , then $[K : F]$ is finite.
 - (e) If $F \subseteq E \subseteq K$ is a tower of fields and K is normal over F , then E is normal over F .
 - (f) If $F \subseteq E \subseteq K$ is a tower of fields and K is normal over F , then K is normal over E .
 - (g) If $F \subseteq E \subseteq K$ is a tower of fields, E is normal over F and K is normal over E , then K is normal over F .
 - (h) If $F \subseteq E \subseteq K$ is a tower of fields and K is separable over F , then E is separable over F .
 - (i) If $F \subseteq E \subseteq K$ is a tower of fields and K is separable over F , then K is separable over E .
 - (j) If $F \subseteq E \subseteq K$ is a tower of fields, E is separable over F and K is separable over E , then K is separable over F .
2. Give an example of an infinite chain $\Omega_1 \subset \Omega_2 \subset \Omega_3 \subset \cdots$ of algebraically closed fields.
3. Let E be an extension field of a field F and $f(x), g(x) \in F[x]$. Prove that a greatest common divisor of f and g in $F[x]$ is also a greatest common divisor of f and g in $E[x]$.
4. Let F be a field and F^* its multiplicative group. Show that the abelian groups $(F, +)$ and (F^*, \cdot) are not isomorphic.
5. Prove that a finite subgroup of the multiplicative group of a field must be cyclic.
6. Show that if F is a finite extension of \mathbb{Q} , then the torsion subgroup of F^* is finite. [Hint: The torsion subgroup consists of roots of unity.]
7. Suppose $F \subset E \subset K$ is any tower of fields and $[K : F]$ is finite. Show that $[K : F] = [K : E][E : F]$.
8. Let K be a field extension of F of degree n and let $f(x) \in F[x]$ be an irreducible polynomial of degree $m > 1$. Show that if m is relatively prime to n , then f has no root in K .
9. **[CORRECTED]**
Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ be an irreducible polynomial of degree greater than 1 in which all roots lie on the unit circle of \mathbb{C} . Prove that $a_i = a_{n-i}$ for all i .
10. Let F be a field extension of the rational numbers.
 - (a) Show that $\{a + b\sqrt{2} \mid a, b \in F\}$ is a field.
 - (b) Give necessary and sufficient conditions for $\{a + b\sqrt[3]{2} \mid a, b \in F\}$ to be a field.
11. Let K be an extension field of F with $a, b \in K$. Let $[F(a) : F] = m$ and $[F(b) : F] = n$ and assume $(m, n) = 1$. Show that $F(a) \cap F(b) = F$ and $[F(a, b) : F] = mn$.

12. Let F , L , and K be subfields of a field M , with $F \subseteq K$ and $F \subseteq L$. Let $[K : F] = k$ and $[L : F] = \ell$.
- Show that $[KL : F] \leq k\ell$.
 - Show that if $(k, \ell) = 1$ then $[KL : F] = k\ell$.
 - Give an example where $[KL : F] < k\ell$.
13. Let K be a finite dimensional extension field of a field F and let G be a group of F -automorphisms of K . Prove that $|G| \leq [K : F]$.
14. Let E be a finite dimensional extension of a field F and let G be a group of F -automorphisms of E such that $[E : F] = |G|$. Show that F is the fixed field of G .
15. Let E be a finite dimensional extension of a field F and let G be a group of F -automorphisms of E . Show that if F is the fixed field of G , then $[E : F] = |G|$.
16. Let F be a field with the property
- (*) If $a, b \in F$ and $a^2 + b^2 = 0$, then $a = 0$ and $b = 0$.
- Show that $x^2 + 1$ is irreducible in $F[x]$.
 - Which of the fields $\mathbb{Z}_3, \mathbb{Z}_5$ satisfy (*)?
17. In each case below a field F and a polynomial $f(x) \in F[x]$ are given. Either prove that f is irreducible over F or factor $f(x)$ into irreducible polynomials in $F[x]$. Find $[K : F]$, where K is a splitting field for f over F .
- $F = \mathbb{Q}, f(x) = x^4 - 5$.
 - $F = \mathbb{Q}(\sqrt{-3}), f(x) = x^3 - 3$.
 - $F = \mathbb{Q}, f(x) = x^3 - x^2 - 5x + 5$.
18. Let \mathbb{Q} be the field of rational numbers. Show that the group of automorphisms of \mathbb{Q} is trivial.
19. Let \mathbb{R} be the field of real numbers. Show that the group of automorphisms of \mathbb{R} is trivial.
20. Let \mathbb{R} be the field of real numbers. Show that if $f(x)$ is an irreducible polynomial over \mathbb{R} , then f is of degree 1 or 2.
21. Let F be a field and p a prime. Let $G = \{c \in F \mid c^{p^n} = 1 \text{ for some positive integer } n\}$.
- Show that G is a subgroup of the multiplicative group of F .
 - Prove that either G is a cyclic group or G is isomorphic to $\mathbb{Z}(p^\infty)$, the Prüfer group for the prime p .
22. Let E be a finite dimensional extension of a field F and let G be a group of F -automorphisms of E . Show the following.
- If $e \in E$ then $G_e = \{\sigma \in G \mid \sigma(e) = e\}$ is a subgroup of G .
 - $[G : G_e] \leq [F(e) : F]$.
 - If F is the fixed field of G and e_1, e_2, \dots, e_n are the distinct images of e under G , then $f(x) = (x - e_1)(x - e_2) \cdots (x - e_n)$ is the minimal polynomial of e over F .
23. Find the minimal polynomial of $\alpha = \sqrt{3 + \sqrt{7}}$ over the field \mathbb{Q} of rational numbers, and *prove* it is the minimal polynomial.

24. Find the minimal polynomial of $\alpha = \sqrt{5 + \sqrt{3}}$ over the field \mathbb{Q} of rational numbers, and *prove* it is the minimal polynomial.
25. Find the minimal polynomial of $\alpha = \sqrt{3 + 2\sqrt{2}}$ over the field \mathbb{Q} of rational numbers, and *prove* it is the minimal polynomial.
26. Find the minimal polynomial of $\alpha = \sqrt[3]{2 + \sqrt{2}}$ over the field \mathbb{Q} of rational numbers, and *prove* it is the minimal polynomial.
27. Let F be a field. Show that F is algebraically closed if and only if every maximal ideal of $F[x]$ has codimension 1.

Algebraic Extensions

28. Let $F \subseteq K$ be fields and let $\alpha \in K$ be algebraic over F with minimal polynomial $f(x) \in F[x]$ of degree n . Show that $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F .
29. Show that if K is finite dimensional field extension of F , then K is algebraic over F .
30. Let F be a field, let $E = F(a)$ be a simple extension field of F , and let $b \in E - F$. Prove that a is algebraic over $F(b)$.
31. Let K be an extension field of the field F such that $[K : F]$ is odd. Show that if $u \in K$ then $F(u) = F(u^2)$.
32. Let K be a finite degree extension of the field F such that $[K : F]$ is relatively prime to 6. Show that if $u \in K$ then $F(u) = F(u^3)$.
33. Let F be a field, $f(x)$ an irreducible polynomial in $F[x]$, and α a root of f in some extension of F . Show that if some odd degree term of $f(x)$ has a non-zero coefficient, then $F(\alpha) = F(\alpha^2)$.
34. Let $f(x)$ and $g(x)$ be irreducible polynomials in $F[x]$ of degrees m and n , respectively, where $(m, n) = 1$. Show that if α is a root of $f(x)$ in some field extension of F , then $g(x)$ is irreducible in $F(\alpha)[x]$.
35. Let K be an extension field of F and let α be an element of K . Show that if $F(\alpha) = F(\alpha^2)$, then α is algebraic over F .
36. Let K be an extension field of F and let α be an element of K . Show that the following are equivalent:
 - (i) α is algebraic over F ,
 - (ii) $F(\alpha)$ is a finite dimensional extension of F ,
 - (iii) α is contained in a finite dimensional extension of F .
37. Let α be algebraic over \mathbb{Q} with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ and set $F = \mathbb{Q}(\alpha)$. Prove that if $f(x) \in \mathbb{Q}[x]$ is irreducible over \mathbb{Q} , then one of the following occurs:
 - (i) $f(x)$ remains irreducible in $F[x]$;
 - (ii) $f(x)$ is a product of two irreducible polynomials in $F[x]$ of equal degree.

38. Let $F \subset E \subset K$ be a tower of fields such that $K = F(\alpha)$ with α algebraic over F . Prove that if $f(x) \in F[x]$ is the minimal polynomial of α over F and $F \neq E$, then $f(x)$ is not irreducible in $E[x]$.
39. Let E be an extension field of F and $A = \{e \in E \mid e \text{ is algebraic over } F\}$.
- Show that A is a subfield of E containing F .
 - Show that if $\sigma : E \rightarrow E$ is a one-to-one F -homomorphism, then $\sigma(A) = A$.
40. Show that if p_1, \dots, p_n, p_{n+1} are distinct prime numbers, then $\sqrt{p_{n+1}}$ is not an element of the field $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$.
41. Let α_1, α_2 , and α_3 be real numbers such that $(\alpha_i)^2 \in \mathbb{Q}$ for each i , and let $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Show that $\sqrt[3]{2}$ is not in K .
42. Let $F \subseteq L \subseteq K$ with $[L : F]$ finite, and let α be an element of K . Show that α is algebraic over L if and only if α is algebraic over F .
43. Show that if K is algebraic over F and $\sigma : K \rightarrow K$ is an F -monomorphism, then σ is onto.
44. Suppose K is an algebraic extension field of a field F such that there are only finitely many intermediate fields between F and K . Show that K is a simple extension of F .
45. Let K be a simple algebraic extension of a field F . Show that there are only finitely many intermediate fields between F and K .
46. Suppose E is an algebraic extension of F and \bar{E} is an algebraic closure of E . Show that \bar{E} is an algebraic closure of F .
47. Let α be algebraic over the field F with minimal polynomial $f(x) \in F[x]$ and let $K = F[\alpha]$. Show that if $\sigma : F \rightarrow L$ is a field monomorphism and $\beta \in L$ is a root of $f^\sigma(x) \in L[x]$, then σ has a unique extension $\hat{\sigma} : K \rightarrow L$ satisfying $\hat{\sigma}(\alpha) = \beta$.
48. Suppose E_1 and E_2 are algebraic closures of a field F . Show that there is an F -isomorphism $\sigma : E_1 \rightarrow E_2$.
49. (a) Show that for every prime p and every positive integer n there is an irreducible polynomial of degree n over the field \mathbb{F}_p of p elements.
- (b) Show that for every positive integer n there is an irreducible polynomial of degree n over the field \mathbb{Q} of rational numbers.

Normality and Splitting Fields

50. Let K be an extension field of F . Show that the following are equivalent.
- Each irreducible polynomial in $F[x]$ with one root in K has all its roots in K .
 - K is obtained from F by adjoining all roots of a set of polynomials in $F[x]$.
 - Every F -isomorphism of K in a fixed algebraic closure is an F -automorphism.
51. Let K be the splitting field of $x^2 + 2$ over \mathbb{Q} . Prove or disprove that $i = \sqrt{-1}$ is an element of K .

52. Let K be the splitting field of $x^3 - 5$ over \mathbb{Q} . Prove or disprove that $i = \sqrt{-1}$ is an element of K .
53. Let Ω be a fixed algebraic closure of F and $K \subseteq \Omega$ an algebraic extension of F . Show that K is a normal extension of F if and only if every F -isomorphism $\varphi : K \rightarrow K' \subseteq \Omega$ is an F -automorphism.
54. Let F be a field and E a splitting field of the irreducible polynomial $f(x) \in F[x]$. Show that if $c, d \in F$ and $c \neq 0$, then the polynomial $f(cx + d)$ splits in $E[x]$.

Separability

55. Show that if K is a separable extension of F and L is a field with $F \subseteq L \subseteq K$, then L is a separable extension of F and K is a separable extension of L .
56. Let $f(x) \in F[x]$ be a polynomial, and let $f'(x)$ denote its formal derivative in $F[x]$. Prove that $f(x)$ has distinct roots in any extension field of F if and only if $\gcd(f(x), f'(x)) = 1$.
57. Show that if K is a finite dimensional separable extension of F , then $K = F(u)$ for some u in K .
58. Let F be a field and let $f(x) = x^n - x \in F[x]$. Show that if $\text{char } F = 0$ or if $\text{char } F = p$ and $p \nmid n - 1$, then f has no multiple root in any extension of F .
59. Show that if F is a field of characteristic 0 then every algebraic extension of F is separable.
60. Show that if F is a finite field then every algebraic extension of F is separable.
61. Let F be a field of characteristic p and let x be an indeterminate over F .
- Show that $F(x^p)$ is a proper subfield of $F(x)$.
 - Show that $F(x)$ is a splitting field for some polynomial over $F(x^p)$.
 - Show that the only automorphism of $F(x)$ fixing $F(x^p)$ is the identity automorphism.
62. Let F be a field and $f(x) \in F[x]$ an irreducible polynomial. Prove that there is a prime p , an integer $a \geq 0$ and a separable polynomial $g(x) \in F[x]$ such that $f(x) = g(x^{p^a})$.
63. Let K be an arbitrary separable extension of F . Show that if every element of K is a root of a polynomial in $F[x]$ of degree less than or equal to n , then K is a simple extension of F of degree less than or equal to n .
64. Let F be a field and let $f(x) \in F[x]$ have splitting field K . Show that if the degree of f is a prime p and $[K : F] = tp$ for some integer t , then
- $f(x)$ is irreducible over F and
 - if $t > 1$ then K is a separable extension of F .
65. Let x and y be independent indeterminates over \mathbb{Z}_p , $K = \mathbb{Z}_p(x, y)$, and $F = \mathbb{Z}_p(x^p, y^p)$.
- Show that $[K : F] = p^2$
 - Show that K is not a simple extension of F .

66. A field F is called *perfect* if every element of an algebraic closure of F is separable over F . Let F be a field of characteristic p . Show that the following are equivalent.
- (i) The field F is perfect.
 - (ii) For every $\epsilon \in F$ there exists a $\delta \in F$ such that $\delta^p = \epsilon$.
 - (iii) The map $a \mapsto a^p$ is an automorphism of F .

67. Show that every field of characteristic 0 is perfect.

68. Show that every finite field is perfect.

69. Let $F \subseteq K$ be fields having characteristic p and assume that K is a normal algebraic extension of F . Prove that there exists a field E with $F \subseteq E \subseteq K$, E/F purely inseparable, and K/E separable.

70. Let E be a field and let G be a finite group of automorphisms of E . Let F be the fixed field of G . Prove that E is a separable algebraic extension of F .

71. Let G be a finite group of automorphisms of the field K and set

$$F = \{\alpha \in K \mid \alpha^\sigma = \alpha \text{ for all } \sigma \in G\}.$$

Show that every element of K is separably algebraic over F of degree at most $|G|$.

72. Let p be a prime and let $F = \mathbb{Z}_p(x)$ be the field of fractions of $\mathbb{Z}_p[x]$. Let E be the splitting field of $f(y) = y^p - x$ over F .
- (a) Show that $[E : F] = p$.
 - (b) Show that $|\text{Aut}_F(E)| = 1$.
 - (c) What conclusion can you draw from (a) and (b)?

73. Let $K = F(u)$ be a separable extension of F with $u^m \in F$ for some positive integer m . Show that if the characteristic of F is p and $m = p^t r$, then $u^r \in F$.

74. If K is an extension of a field F of characteristic $p \neq 0$, then an element u of K is called *purely inseparable* over F if $u^{p^t} \in F$ for some t . Show that the following are equivalent.

- (i) u is purely inseparable over F .
- (ii) u is algebraic over F with minimal polynomial $x^{p^n} - a$ for some $a \in F$ and integer n .
- (iii) u is algebraic over F and its minimal polynomial factors as $(x - u)^m$.

75. Show that every purely inseparable field extension is a normal extension.

76. Let K be an extension of a field F of characteristic $p \neq 0$. Show that an element u of K is both separable and purely inseparable if and only if $u \in F$.

77. Let $\mathbb{Z}_2(x)$ be the field of fractions of the polynomial ring $\mathbb{Z}_2[x]$. Construct an extension of $\mathbb{Z}_2(x)$ that is neither separable nor purely inseparable.

Galois Theory

78. State the Fundamental Theorem of Galois Theory.
79. Let K be a finite Galois extension of F with Galois group G . Suppose that E_1 and E_2 are intermediate extensions satisfying $E_1 \subset E_2$, and let $H_1 \supset H_2$ be the corresponding subgroups of G . Prove that E_2 is a normal extension of E_1 if and only if H_2 is a normal subgroup of H_1 , and when this happens, the Galois group of E_2 over E_1 is isomorphic to H_1/H_2 .
80. Let K be a finite Galois extension of F with Galois group $G = \text{Gal}(K/F)$. Let E be an intermediate field that is normal over F . Prove that $\text{Gal}(K/E) \trianglelefteq G$ and $G/\text{Gal}(K/E) \cong \text{Gal}(E/F)$.
81. Let K be a finite algebraic extension of F and let G be the group of all F -automorphisms of K . Let $\mathcal{F}(G) = \{u \in K \mid \sigma(u) = u \text{ for all } \sigma \in G\}$. Show that K is both separable and normal (i.e. Galois) over F if and only if $\mathcal{F}(G) = F$.
82. Let K be a finite dimensional extension field of L and let $\sigma : L \rightarrow F$ be an embedding of L into a field F . Prove that there are at most $[K : L]$ extensions of σ to embeddings of K into F .
83. Let K be an extension field of F and let F' be the fixed field of the group of F -automorphisms of K . Show that K is a Galois extension of F' .
84. Let K be a finite normal extension of F and let E be the fixed field of the group of all F -automorphisms of K . Show that the minimal polynomial over F of each element of E has only one distinct root.
85. Let E be a splitting field over F of a separable polynomial $f(x)$ in $F[x]$ and $G = \text{Gal}(E/F)$. Show that $\{e \in E \mid \sigma(e) = e \text{ for all } \sigma \in G\} = F$.
86. Let K be a Galois extension of F with $|\text{Gal}(K/F)| = 12$. Prove that there exists a subfield E of K containing F with $[E : F] = 3$. Does a subextension necessarily exist satisfying $[E : F] = 2$? Explain.
87. Suppose $K = F(\alpha)$ is a proper Galois extension of F and assume there exists an element σ of $\text{Gal}(K/F)$ satisfying $\sigma(\alpha) = \alpha^{-1}$. Show that $[K : F]$ is even and that $[F(\alpha + \alpha^{-1}) : F] = \frac{1}{2}[K : F]$.
88. Let K be a finite Galois extension of F of characteristic 0. Show that if $\text{Gal}(K/F)$ is a non-trivial 2-group, then there is a quadratic extension of F contained in K .
89. Let G be a finite group. Show that there is an algebraic extension F of the field \mathbb{Q} of rational numbers and a Galois extension K of F such that $G \cong \text{Gal}(K/F)$.
90. (a) Find the Galois group of $x^3 - 2$ over \mathbb{Q} and demonstrate the Galois correspondence between the subgroups of the Galois group and the subfields of the splitting field.
(b) Find all automorphisms of $\mathbb{Q}(\sqrt[3]{2})$. Is there an $f(x) \in \mathbb{Q}[x]$ with splitting field $\mathbb{Q}(\sqrt[3]{2})$? Explain.
91. Let F be any field and let $f(x) = x^n - 1 \in F[x]$. Show that if K is the splitting field of $f(x)$ over F , then K is separable over F (hence Galois) and that $\text{Gal}(K/F)$ is abelian.

92. Let η_7 be a complex primitive 7th root of unity and let $K = \mathbb{Q}(\eta_7)$. Find $\text{Gal}(K/\mathbb{Q})$ and express each intermediate field F between \mathbb{Q} and K as $F = \mathbb{Q}(\beta)$ for some $\beta \in K$.
93. Let η be a complex primitive 7th root of unity and let $K = \mathbb{Q}(\eta)$, where \mathbb{Q} is the field of rational numbers. Show that there is a unique extension F of degree 2 of \mathbb{Q} contained in K and find $q \in \mathbb{Q}$ such that $F = \mathbb{Q}(\sqrt{q})$.
94. Let \mathbb{Q} be the field of rational numbers and η a complex primitive 8th root of unity. Determine $\text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$ and all the intermediate fields between \mathbb{Q} and $\mathbb{Q}(\eta)$.
95. (a) Determine the Galois group of $x^4 - 4$ over the field \mathbb{Q} of rational numbers.
 (b) How many intermediate fields are there between \mathbb{Q} and the splitting field of $x^4 - 4$?
96. **[NEW]**
 Determine the Galois group of $x^4 - 3$ over the field \mathbb{Q} of rational numbers.
97. Determine the Galois group of $x^4 + 2$ over the field \mathbb{Q} of rational numbers.
98. Determine the Galois group of $x^3 + 3x^2 - 1$ over \mathbb{Q} .
99. Show that the Galois group of $x^3 - 5$ over \mathbb{Q} is S_3 and demonstrate the Galois correspondence between the subgroups of S_3 and the subfields of the splitting field. Which subfields are normal over \mathbb{Q} ?
100. Let K be a splitting field for $x^5 - 2$ over \mathbb{Q} .
 (a) Determine $[K : \mathbb{Q}]$.
 (b) Show that $\text{Gal}(K/\mathbb{Q})$ is non-abelian.
 (c) Find all normal intermediate extensions F and express as $F = \mathbb{Q}(\alpha)$ for appropriate α .
101. Let \mathbb{Q} be the field of rational numbers and E the splitting field (in the field of complex numbers) of $x^4 - 2$.
 (a) Find $|\text{Gal}(E/\mathbb{Q})|$.
 (b) Let $\sigma \in \text{Gal}(E/\mathbb{Q})$ be such that $\sigma(\alpha) = \bar{\alpha}$ for all $\alpha \in E$ (where $\bar{\alpha}$ is the complex conjugate of α). Find $\text{Inv}(\langle \sigma \rangle) = \{\alpha \in E \mid \sigma(\alpha) = \alpha\}$.
 (c) Is $\langle \sigma \rangle$ a normal subgroup of $\text{Gal}(E/\mathbb{Q})$?
102. Let $f(x) = x^4 + 4x^2 + 2$ and let K be the splitting field of f over \mathbb{Q} . Show that the Galois group of K over \mathbb{Q} is cyclic of order 4.
103. Let F be the field of 2 elements and K a splitting field of $f(x) = x^6 + x^3 + 1$ over F .
 (a) Show that if r is a root of f , then $r^9 = 1$ but $r^3 \neq 1$.
 (b) Show that f is irreducible over F .
 (c) Find $\text{Gal}(K/F)$ and express each intermediate field between F and K as $F(b)$ for appropriate b in K .
104. Let K be a Galois extension of \mathbb{Q} whose Galois group is isomorphic to S_5 . Prove that K is the splitting field of some polynomial of degree 5 over \mathbb{Q} .
105. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n with roots $\alpha_1, \dots, \alpha_n$. Show that $\sum_{i=1}^n \frac{1}{\alpha_i}$ is a rational number.

106. Let $\alpha = \sqrt{2} + \sqrt{3}$ and let $E = \mathbb{Q}(\alpha)$.
- Find the minimal polynomial $m(x)$ of α over \mathbb{Q} and $|E : \mathbb{Q}|$.
 - Find the splitting field of $m(x)$ over \mathbb{Q} and all intermediate fields, and find its Galois group over \mathbb{Q} and all its subgroups.
107. Let $u = \sqrt{2 + \sqrt{2}}$, $v = \sqrt{2 - \sqrt{2}}$, and $E = \mathbb{Q}(u)$, where \mathbb{Q} is the field of rational numbers.
- Find the minimal polynomial $f(x)$ of u over \mathbb{Q} .
 - Show $v \in E$. Hence conclude that E is a splitting field of $f(x)$ over \mathbb{Q} .
 - Determine the Galois group of E over \mathbb{Q} .
108. Let $\alpha = \sqrt{5 + 2\sqrt{5}}$. Show that $\mathbb{Q}(\alpha)$ is a cyclic Galois extension of \mathbb{Q} of degree 4. Find all fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\alpha)$.
[Hint: Show that $f(x) = x^4 - 10x^2 + 5$ is the minimal polynomial of α over \mathbb{Q} and that the roots of f are $\pm\alpha, \pm\frac{\sqrt{5}}{\alpha}$.]
109. Let p be a prime such that there is a positive integer d with $p = 1 + d^2$ and let $\alpha = \sqrt{p + d\sqrt{p}}$. Show that $\mathbb{Q}(\alpha)$ is a cyclic Galois extension of \mathbb{Q} of degree 4. Find all fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\alpha)$.
[Hint: Show that $f(x) = x^4 - 2px^2 + p$ is the minimal polynomial of α over \mathbb{Q} and that the roots of f are $\pm\alpha, \pm\frac{\sqrt{p}}{\alpha}$.]
110. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 with exactly 2 real roots. Show that the Galois group of f is either S_4 or the dihedral group of order 8.
111. Let $f(x) = x^4 + ax^3 + bx^2 + ax + 1 \in \mathbb{Q}[x]$ and let F be a splitting field over \mathbb{Q} . Show that if α is a root of f then $1/\alpha$ is also a root, and $|\text{Gal}(F/\mathbb{Q})| \leq 8$.
112. Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial of degree 4 with distinct roots $\alpha_1, \alpha_2, \alpha_3$, and α_4 . Let K be a splitting field for f over F and assume $\text{Gal}(K/F) \cong S_4$. Find $\text{Gal}(K/F(\beta))$, where $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$.
113. Let E be a finite dimensional Galois extension of a field F and let $G = \text{Gal}(E/F)$. Suppose that G is an abelian group. Prove that if K is any field between E and F , then K is a Galois extension of F .
114. Let K be a finite Galois extension of F and let E be an intermediate field which is normal over F . For an element σ of $\text{Gal}(K/F)$ and $g(x) = e_0 + e_1x + \cdots + e_mx^m$ in $E[x]$, denote $\sigma g(x) = \sigma(e_0) + \sigma(e_1)x + \cdots + \sigma(e_m)x^m$. For a fixed element α of K , let $f(x) \in E[x]$ be the minimal polynomial of α over E . Show the following.
- $\sigma(\alpha)$ is a root of $\sigma f(x)$.
 - If $f_1(x), f_2(x), \dots, f_n(x)$ are all the distinct elements of $\{\sigma f(x) \mid \sigma \in \text{Gal}(K/F)\}$, then $h(x) = f_1(x)f_2(x)\cdots f_n(x)$ is in $F[x]$.
 - $h(x)$ is the minimal polynomial of α over F .
115. Let K be a Galois extension of k and let $k \subseteq F \subseteq K$ and $k \subseteq L \subseteq K$.
- Show that $\text{Gal}(K/LF) = \text{Gal}(K/L) \cap \text{Gal}(K/F)$.
 - Show that $\text{Gal}(K/L \cap F) = \langle \text{Gal}(K/L), \text{Gal}(K/F) \rangle$.

116. Let $\overline{\mathbb{Q}}$ be the algebraic closure of \mathbb{Q} and let α be an element of $\overline{\mathbb{Q}}$ not in \mathbb{Q} .
- Show that there is a field $M \subseteq \overline{\mathbb{Q}}$ that is maximal with respect to the property that $\alpha \notin M$.
 - Show that any finite Galois extension of M has cyclic Galois group.
 - Show that any finite extension of M is a Galois extension.
117. Let E be a finite dimensional Galois extension of a field F and let $G = \text{Gal}(E/F)$. For $e \in E$ let $G(e) = \{\sigma(e) \mid \sigma \in G\}$. Let e_1, e_2, \dots, e_n be all the distinct elements of $G(e)$.
- Prove that $f(x) = (x - e_1)(x - e_2) \cdots (x - e_n)$ is in $F[x]$.
 - Prove that $f(x)$ is irreducible in $F[x]$.
118. Let E be a finite dimensional Galois extension of F of characteristic different from 2. Suppose $\text{Gal}(E/F)$ is a non-cyclic group of order 4. Show that $E = F(\alpha, \beta)$ for some $\alpha, \beta \in E$ with $\alpha^2 \in F$ and $\beta^2 \in F$.

Cyclotomic Extensions

119. Find the 6th, 8th, and 12th cyclotomic polynomials over \mathbb{Q} .
120. Let α be a complex primitive 43rd root of 1. Prove that there is an extension field F of the rational numbers such that $[F(\alpha) : F] = 14$.
121. Let m be an odd integer and let η_m, η_{2m} be a complex primitive m -th, $2m$ -th root of unity, respectively. Show that $\mathbb{Q}(\eta_m) = \mathbb{Q}(\eta_{2m})$.
122. Let $(m, n) = 1$, and if i is any positive integer let η_i denote a complex primitive i -th root of unity. Show that $\mathbb{Q}(\eta_{mn}) = \mathbb{Q}(\eta_m)\mathbb{Q}(\eta_n)$ and $\mathbb{Q}(\eta_m) \cap \mathbb{Q}(\eta_n) = \mathbb{Q}$.
123. Let ϵ be the complex number $\cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$, where n is a positive integer. Show
- ϵ is algebraic over the field \mathbb{Q} of rational numbers,
 - if $\Phi_n(x)$ is the minimal polynomial of ϵ over \mathbb{Q} , then $\mathbb{Q}(\epsilon)$ is a splitting field of $\Phi_n(x)$ over \mathbb{Q} ,
 - the Galois group of $\mathbb{Q}(\epsilon)$ over \mathbb{Q} is isomorphic to the group of units of \mathbb{Z}_n .
124. Let ϵ be a primitive n -th root of unity over \mathbb{Q} , where $n > 2$, and let $\alpha = \epsilon + \epsilon^{-1}$. Prove that α is algebraic over \mathbb{Q} of degree $\varphi(n)/2$.

Finite Fields

125. Prove that the multiplicative group of a finite field must be cyclic.
126. Prove that any finite extension of a finite field must be a simple extension.
127. Show that any two finite fields of the same order are isomorphic.
128. Let F be an extension of \mathbb{Z}_p of degree n . Show that F is a Galois extension and $\text{Gal}(F/\mathbb{Z}_p)$ is cyclic of order n .
129. Show that every finite extension of a finite field is a Galois extension.

130. Show that every algebraic extension of a finite field is separable.
131. Show that every finite field is perfect. (Recall that a field F of characteristic p is called *perfect* if the map $\alpha \mapsto \alpha^p$ is a surjection on F .)
132. Let $f(x) \in \mathbb{Z}_p[x]$ be irreducible of degree m . Show that $f|(x^{p^n} - x)$ if and only if $m|n$.
133. Let p be a prime. Show that the field of p^a elements is a subfield of the field of p^b elements if and only if $a|b$.
134. Let p be a prime and \mathbb{F}_p the field of p elements. Show that for every positive integer n , there is an irreducible polynomial of degree n over \mathbb{F}_p .
135. Let F be a finite field. Show that the product of all the non-zero elements of F is -1 .
136. Let \mathbb{F}_q be the field of q elements and let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$. Show that if α is a root of $f(x)$, then α^q is also a root of $f(x)$.
137. Let E and F be subfields of a finite field K . Show that if E is isomorphic to F then $E = F$.
138. Let E and F be finite subfields of a field K . Show that if E and F have the same number of elements, then $E = F$.
139. Let \mathbb{F}_p be the field of p elements and let K be an extension of \mathbb{F}_p of degree n . Show that the set of subfields of K is linearly ordered (i.e., for every pair of subfields L_1, L_2 , either $L_1 \subseteq L_2$ or $L_2 \subseteq L_1$) if and only if n is a prime power.
140. Let α be a root of $x^2 + 1$ in an extension of \mathbb{Z}_3 , $K = \mathbb{Z}_3(\alpha)$, and let $f(x) = x^4 + 1 \in \mathbb{Z}_3[x]$.
- Show that f splits over K .
 - Find a generator β of the multiplicative group K^* of K .
 - Express the roots of f in terms of β .
141. Let $K = \mathbb{Z}_3(\sqrt{2})$ and let $f(x) = x^4 + x^3 + x + 2 \in \mathbb{Z}_3[x]$.
- Show that f splits over K .
 - Find a generator α of the multiplicative group K^* of K .
 - Express the roots of f in terms of α .
142. Let $\mathbb{F} = \mathbb{F}_{81}$ be the field of 81 elements.
- Find all subfields of \mathbb{F} .
 - Determine the number of primitive elements for \mathbb{F} over the field \mathbb{F}_3 of 3 elements (i.e., elements α of \mathbb{F} such that $\mathbb{F} = \mathbb{F}_3(\alpha)$).
 - Find the number of generators for the multiplicative group \mathbb{F}^* of \mathbb{F} (i.e., elements β of \mathbb{F} such that $\langle \beta \rangle = \mathbb{F}^*$).
143. Let $f(x) = x^4 + x^3 + 4x - 1 \in \mathbb{Z}_5[x]$.
Find the Galois group of the splitting field of f over \mathbb{Z}_5 .

Cyclic Extensions

144. Let K be a field of characteristic $p \neq 0$ and let $K_p = \{u^p - u : u \in K\}$. Show that K has a cyclic extension of degree p if and only if $K \neq K_p$.
145. Let p be a prime and F the field of fractions of $\mathbb{Z}_p[x]$. If E is the splitting field of $y^p - y - x$ over F , determine the Galois group of E over F .
146. Let n be a positive integer and let F be a field of characteristic 0 containing a primitive n -th root of unity. Let a be an element of F such that a is not an m -th power of an element of F for any $1 \neq m|n$. Show that if α is any root of $x^n - a$, then $F(\alpha)$ is a cyclic extension of F of degree n .
147. Let F be a field that contains a primitive n th root of unity and let $K = F(t)$, the field of fractions of the polynomial ring $F[t]$. Let $L = F(t^n) \subseteq K$. Prove that K is a Galois extension of L and that the Galois group is cyclic of order n .
148. Let F be a field of characteristic p . Fix $c \in F$ and let $f(x) = x^p - x + c \in F[x]$. Prove that if α is a root of $f(x)$ in some extension field, then so is $\alpha + 1$. Use this to prove that if K is the splitting field of $f(x)$ over F , then either $K = F$ and $f(x)$ splits completely over F , or $[K : F] = p$ and $f(x)$ is irreducible over F . (Use Galois groups.)

Radical Extensions and Solvability By Radicals

149. An extension K of F is called a *radical extension* if there is a tower of fields

$$F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq \cdots \subseteq F(u_1, \dots, u_n) = K$$

such that for $i = 1, \dots, n$, $u_i^{m_i} \in F(u_1, \dots, u_{i-1})$ for some positive integer m_i .

- (a) Give an example of a radical extension that is not separable.
- (b) Give an example of a radical extension that is not normal.
150. Let F be a radical extension of K . Show that there is a radical extension N of K with $N \supseteq F \supseteq K$ and N normal over K .
151. Let F be a finite field of characteristic p . Show that if $f \in F[x]$ is an irreducible polynomial and the degree of f is less than p , then $f(x) = 0$ is solvable by radicals.
152. Let x_1, \dots, x_n be indeterminates over a field F and let s_1, \dots, s_n be the elementary symmetric functions of the x_i . Show that $[F(x_1, \dots, x_n) : F(s_1, \dots, s_n)] = n!$.

Transcendental Extensions

153. Let x be an indeterminate over the field F . Show that an element of $F(x)$ is algebraic over F if and only if it is an element of F .
154. Let $F \subseteq E$ be fields with $E = F(\alpha)$, where α is transcendental over F . Show that if $\beta \in E - F$, then $[E : F(\beta)]$ is finite.

155. Let F be a field, $F[x]$ the ring of polynomials over F in the indeterminate x , and $E = F(x)$ the field of fractions of $F[x]$.
- (a) Show that if σ is an automorphism of E such that $\sigma(u) = u$ for all $u \in F$, then $\sigma(x) = \frac{ax + b}{cx + d}$ for some $a, b, c, d \in F$ with $ad - bc \neq 0$.
- (b) Determine the group $\text{Aut}_F(E)$ of F -automorphisms of E .
156. Let K be an extension field of F and let $\alpha \in K$ be transcendental over F . Show that if $\beta \in K$ is algebraic over $F(\alpha)$, then there is a nonzero polynomial $p(x, y) \in F[x, y]$ such that $P(\alpha, \beta) = 0$.