

Algebra Syllabus

Department of Mathematics

University of Colorado

Group Theory. Basic definitions and examples, lattice of subgroups/normal subgroups, quotient groups, isomorphism theorems, the characterization of products, Lagrange's Theorem, Cauchy's Theorem, Cayley's Theorem, the structure of finitely generated abelian groups, group actions, the class equation, Sylow's Theorems, the Jordan Hölder Theorem, simple groups, solvable groups, semidirect products, free groups, presentations of groups.

Ring Theory. Basic definitions and examples, lattice of subrings/ideals, quotient rings, chain conditions, rings of fractions, Chinese Remainder Theorem, Euclidean domains, PID's, UFD's, polynomial rings, irreducibility criteria for polynomials.

Modules and Linear Algebra. Basic definitions and examples, lattice of submodules, quotient modules, tensor products of modules, the matrix of a linear transformation, minimal polynomial of a transformation, Cayley-Hamilton Theorem, trace and determinant, dual spaces, modules over a PID, rational canonical form, Jordan canonical form.

Field Theory. Basic definitions and examples, field extensions, simple extensions, algebraic extensions, transcendental extensions, separable and inseparable extensions, cyclotomic extensions, solution of the Greek construction problems, splitting fields and normality, algebraic closure, the Galois correspondence, Galois groups of extensions/polynomials, solvable and radical extensions, the insolvability of the quintic, Fundamental Theorem of Algebra, Casus Irreducibilis, finite fields, Frobenius endomorphism.

Miscellaneous. Axiom of choice and Zorn's lemma, universal constructions (products, coproducts), lattices.

References.

M. Artin, *Algebra*
D. Dummit and R. Foote, *Abstract Algebra*
T. Hungerford, *Algebra*
N. Jacobson, *Basic Algebra I*
S. Lang, *Algebra*

1. Let G be a nonabelian finite simple group, and let p be a prime divisor of its order $|G|$. Show that if the number of Sylow p -subgroups of G is n , then $|G|$ divides $n!$.

2. Let G be a finite solvable group. Show that
 - (a) G has a nontrivial abelian normal subgroup of prime power order, and
 - (b) Every maximal proper subgroup of G has prime power index in G .

3. Let R be a UFD such that any ideal generated by two elements of R is principal. Prove that R is a PID. [Hint: If $a \in I$ is to generate the ideal I , consider what the factorization of a must look like.]

4. Let A be an $n \times n$ matrix over \mathbb{C} such that $\text{tr}(A^k) = 0$ for all $k > 0$. Show that $A^n = 0$. (The trace $\text{tr}(M)$ of a matrix M is the sum of its diagonal entries.)

5. Find the splitting field of $x^4 + x^3 + 1$ over the 32-element field.

6. True or false? Justify your answer.
 - (a) Every field extension of degree 2 is Galois.
 - (b) Every algebraically closed field is infinite.
 - (c) If $\alpha = \sqrt[5]{2+i} + \sqrt[5]{2-i}$, then $\text{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q}) \cong S_5$.

1. Prove that in a group of order 12, any two elements of order 6 must commute.

2. Show that any group of order 105 has an element of order 35.

3. Let R be an integral domain in which every nonzero element factors into a product of finitely many irreducible elements up to a unit. For any $a, b \in R - \{0\}$, define the ideal

$$I_{a,b} = \{x \in R : ax \in (b)\},$$

where (b) is the ideal of R generated by the element b . Then show that R is a UFD $\iff I_{a,b}$ is principal for any $a, b \in R - \{0\}$.

4. Let R be an associative ring with $1 \neq 0$ and let $N \subseteq M$ be left R -modules. Suppose that N and M/N are Noetherian. Then show that M is Noetherian.

5. Let \circ be a binary operation on the field \mathbb{R} of real numbers. Show that \mathbb{R} has a countable subfield F with the following properties:

- (i) Every positive element of F has a square root.
- (ii) Every polynomial of odd degree over F has a root.
- (iii) F is closed under \circ .

6. Determine the splitting field of the polynomial $x^5 + 2x^4 + 5x^2 + x + 4$ over \mathbb{F}_{11} and its Galois group.

1. There exists an injective group homomorphism $\sigma : S_4 \rightarrow A_7$ given by

$$\begin{aligned}\sigma((12)) &= (12)(56), \\ \sigma((23)) &= (23)(56), \\ \sigma((34)) &= (34)(56).\end{aligned}$$

List the elements in one Sylow 2-subgroup of S_4 and hence, or otherwise, write down a Sylow 2-subgroup of A_7 . Deduce that A_7 contains precisely 315 Sylow 2-subgroups, each of which is self-normalizing. [Hint: each Sylow 2-subgroup of A_7 contains precisely two elements of cycle type $(4,2,1)$.]

2. Classify up to isomorphism all groups of order 8. (Your argument should contain full proofs, although you may use general theorems without proof if you state them clearly.)

3. Let S be the subring of the field of fractions of $\mathbb{R}[x]$ consisting of those fractions whose denominators are relatively prime to $x^2 + 1$, i.e., of the form $p(x)/q(x)$ with $q(x)$ relatively prime to $x^2 + 1$.

- What are the units of S ?
- Identify the ideals of S .
- Is S a unique factorization domain? Explain.
- If \mathbb{R} is replaced by \mathbb{C} and the set of rational functions corresponding to S constructed, would it have a unique maximal ideal? Explain.

4. Let R be a ring with identity 1, and let $f \in R$ be an idempotent (i.e., $f^2 = f$).

- Show that $Rf = \{rf : r \in R\}$ is a projective left R -module under the action $r_1 \cdot (rf) = (r_1r)f$.
- Now let $R = M_2(\mathbb{C})$, and let M be the left R -module

$$M = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{C} \right\}$$

with the usual action. Prove that M is projective.

5. Let α be a zero of the polynomial $p(x) = x^3 - x - 1$ over \mathbb{Z}_3 in some splitting field.

- Express the multiplicative inverse of α as a polynomial of minimum degree in α .
- Express the other zeros of $p(x)$ as polynomials of minimum degree in α .
- What is the minimal polynomial $q(x)$ for α^2 ?
- Express the other zeros of $q(x)$ as polynomials of minimum degree in α .

6. Let $f(x) = x^3 - 5 \in \mathbb{Q}[x]$.

- Find a splitting field for f over \mathbb{Q} .
- Find the Galois group for f .
- Find all proper, nontrivial subgroups of this Galois group and the fields to which they correspond according to the fundamental theorem of Galois theory.

1. Show that if G is a simple group of order $4pq$, where p and q are distinct odd primes, then $|G| = 60$.

2. Let G be a non-trivial finite group. Show that if $M \cap N = \{1\}$ whenever M and N are distinct maximal subgroups of G , then some maximal subgroup of G is normal. (Recall that a subgroup of a group is called *maximal* if it is a proper subgroup not properly contained in any other proper subgroup.)

3. Let \mathbb{F} be a field of order 1024, and let $G = \text{GL}(6, \mathbb{F})$, the group of invertible 6×6 matrices with entries in \mathbb{F} .
 - (a) How many conjugacy classes of G contain an element of order 3?
 - (b) How many conjugacy classes of G contain an element of order 4?

4. Let I be a nonzero ideal in $\mathbb{Z}[i]$. Show that I is a prime ideal if and only if it is a maximal ideal.

5. Let $\mathbb{E} \leq \mathbb{K}$ be a field extension of degree n . Show that if there are more than 2^{n-1} intermediate subfields $\mathbb{E} \leq \mathbb{F} \leq \mathbb{K}$, then there are infinitely many intermediate subfields. (Hint: At some point consider minimal polynomials.)

6. Find the Galois group of $x^6 - 3$ over \mathbb{Q} .

1. Let G be the alternating group A_6 .
 - (a) How many Sylow 2-subgroups does G have?
 - (b) To what well-known group is a Sylow 2-subgroup of G isomorphic?

2. Let G be a group each of whose elements is its own inverse.
 - (a) Prove that G is abelian.
 - (b) If G is finite, what are the only possibilities for its order?
 - (c) Prove that if $|G| > 2$ and is finite, then its automorphism group $\text{Aut}(G)$ is not abelian.

3. Let R be a commutative and associative ring with multiplicative identity $1 \neq 0$ and let I be an ideal of R . Suppose that I is not finitely generated and that the only ideal of R not finitely generated and containing I is I itself. Then show that I is a prime ideal. [Hint: You may want to make use of $J_a := \{r \in R : ra \in I\}$ for $a \in R$.]

4. For any vector spaces V and W over a field k , let $\text{Hom}_k(V, W)$ be the set of k -linear maps (= k -linear transformations) from V to W and let $V^* = \text{Hom}_k(V, k)$.

Now let V and W be finite-dimensional vector spaces over a field k . Then:
 - (a) Show that $\text{Hom}_k(V, W)$ is a vector space over k under the *natural* operations of addition and k -scalar multiplication;
 - (b) Calculate $\dim_k \text{Hom}_k(V, W)$;
 - (c) Calculate $\dim_k (V^* \otimes_k W)$; and
 - (d) Construct an explicit isomorphism to show that $\text{Hom}_k(V, W)$ and $V^* \otimes_k W$ are isomorphic as vector spaces over k .

5. Let K be a field of characteristic $p \neq 0$, and let $f = x^p - x - a \in K[x]$. Show that either f splits (completely) in $K[x]$ or f is irreducible over K .

6. Find a splitting field L/\mathbb{Q} and the Galois group $G = \text{Gal}(L/\mathbb{Q})$ for $f = x^5 - 3 \in \mathbb{Q}[x]$. Find 3 nontrivial, proper subgroups of G and the intermediate fields to which they correspond according to the fundamental theorem of Galois theory.

1. If P is a Sylow p -subgroup of a finite group G , where p is a prime factor of $|G|$, show that
 - (a) For any subgroup H of G containing $N_G(P)$, we have $N_G(H) = H$,
 - (b) $N_G(N_G(P)) = N_G(P)$.

2. Let G be a finite group for which $x^2 = 1$ for all $x \in G$.
 - (a) Prove that G is abelian of order 2^n for some n .
 - (b) Prove that the product of all elements of G is equal to the identity if the order of G is sufficiently large. (Your answer should make it clear what “sufficiently large” means.)

3. (a) Let $n \in \mathbb{Z}$, $n \geq 1$, and let I be the ideal generated by n and x in $\mathbb{Z}[x]$. Show that I is a maximal ideal if and only if n is prime.
 - (b) Show that $\mathbb{Z}[x]$ is not isomorphic, as a ring, to \mathbb{Z} .

Recall that if G is a group, the group ring $\mathbb{Z}G$ is the free \mathbb{Z} -module on G with associative multiplication inherited from the multiplication in G , so that every element in $\mathbb{Z}G$ is uniquely represented by a sum

$$\sum_{g_1 \in G} n_{g_1} g_1$$

with $n_{g_1} \in \mathbb{Z}$, and

$$\sum_{g_1 \in G} n_{g_1} g_1 \sum_{g_2 \in G} n_{g_2} g_2 = \sum_{g \in G} n_g g,$$

where $n_g = \sum_{g_1 g_2 = g} n_{g_1} n_{g_2}$.

- (c) Show that if G is any nontrivial group, the group ring $\mathbb{Z}G$ has at least four units. Deduce that $\mathbb{Z}[x]$ is not isomorphic to any group ring $\mathbb{Z}G$.
-
4. Let S be a commutative ring. We say that S is a *graded ring* if we can decompose S into the direct sum of additive subgroups $S = \bigoplus_{n \geq 0} S_n$, such that for all integers $k, l \geq 0$ we have $S_k S_l \subseteq S_{k+l}$. (For example, if R is a commutative ring, then $S = R[x_1, \dots, x_m]$ is a graded ring, where S_n consists of the elements of total degree n .)
 - (a) If S is a graded ring, verify that S_0 is a subring, and that for every n , S_n is an S_0 -module.
 - (b) Show that if S is a graded ring, then $S_+ = \bigoplus_{n > 0} S_n$ is an ideal of S , and that it is a prime ideal if and only if S_0 is an integral domain.

 5. (a) Let p be an odd prime. By considering the action of the Frobenius automorphism, show that $x^p - x - 1$ is irreducible over \mathbb{F}_p , the field with p elements.
 - (b) Show that the Galois group of $x^5 - 6x - 1$ over \mathbb{Q} is S_5 .

 6. Let p_1, \dots, p_n be distinct odd prime numbers, $m = \prod_{i=1}^n p_i$, and ζ a primitive m^{th} root of unity. Let $K = \mathbb{Q}(\zeta)$. Determine with proof the number of subfields E , $\mathbb{Q} \subseteq E \subseteq K$, with $[E : \mathbb{Q}] = 2$.

1. Show that \mathbb{Q} under addition does not have any proper subgroup of finite index.
2. Show that if G is a group, $|G| = 315$, and G has a normal subgroup of order 9, then G is abelian. You may assume that if $p < q$ are primes such that p does not divide $q - 1$, then a group of order pq is cyclic, and if Z is the center of G and G/Z is cyclic, then G is abelian.
3. (a) (i) Prove that the integral domain $\mathbb{Z}[i]$ (the Gaussian integers) is a Euclidean domain.
(ii) What are its units?
(iii) Give an example of a maximal ideal of $\mathbb{Z}[i]$.
(b) (i) Prove that the integral domain $\mathbb{Z}[x]$ is not a Euclidean domain.
(ii) What are its units?
(iii) Give an example of a maximal ideal of $\mathbb{Z}[x]$.
(c) (i) Prove that the integral domain $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean domain.
(ii) What are its units?
4. Let R be a ring and M a left R -module. For N any submodule of M , define $A(N) = \{a \in R : aN = 0\}$. For J any ideal of R , define $N(J) = \{n \in M : Jn = 0\}$.
 - (a) Prove that $A(N)$ is an ideal of R .
 - (b) Prove that RN is a submodule of M .
 - (c) Prove that $N(J)$ is a submodule of M .
 - (d) Prove: If N and L are submodules of M and $N \subseteq L$, then $A(L) \subseteq A(N)$.
 - (e) Prove: If N_1 and N_2 are submodules of M , then $A(N_1 + N_2) = A(N_1) \cap A(N_2)$.In (f) and (g) assume that R is nilpotent, i.e., there exists a positive integer n such that the product of n elements of R is 0.
 - (f) Prove: If $N \neq 0$, then $RN \neq N$.
 - (g) Prove: If $RM \neq 0$, then M is not the direct sum of RM and $N(R)$.
5. Suppose that $L : K$ is a field extension, $\gamma \in L$ with γ transcendental over K . Suppose that $f \in K[x]$, $\deg f \geq 1$.
 - (a) Show $f(\gamma)$ is transcendental over K .
 - (b) Suppose that $\beta \in L$ with $f(\beta) = \gamma$. Show β is transcendental over K .
 - (c) Suppose that $\alpha \in L$, $\alpha \notin K$, with α algebraic over K . Show $K(\alpha, \gamma)$ is not a simple extension of K .
 - (d) Suppose that α is a root of f , $f \in K[x]$ irreducible of degree n . Prove that $[K[\alpha] : K] = n$ by displaying a basis for $K[\alpha]$ over K ; prove this is indeed a basis. Then prove $K[\alpha]$ is a field.
6. Find a splitting field L and the Galois group G for $x^4 - 2 \in \mathbb{Q}[x]$. Determine the degree of $L : \mathbb{Q}$. Find at least 3 subgroups and the intermediate fields to which they correspond according to the Fundamental Theorem of Galois Theory.

1. Show there is no simple group of order 90.

2. Let p and q be distinct prime numbers with $p \not\equiv 1 \pmod{q}$, and $q \not\equiv 1 \pmod{p}$. Show that every group of order pq is cyclic.

3. Let $d \geq 1$ be an integer. Let $R_d = \{a + b\sqrt{-d} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$, which is a subring of \mathbb{C} . Recall that in a ring with multiplicative identity, an element is called a *unit* if it has a 2-sided multiplicative inverse. Recall also that in an integral domain, an element which is nonzero and not a unit is called *irreducible* if whenever it is written as a product of two elements, one of these elements is a unit.
 - (a) Show that complex conjugation restricts to an automorphism of R_d .
 - (b) Show that ± 1 are the only units of R_d if $d > 1$.
 - (c) Show that $2 + \sqrt{-5}$, $2 - \sqrt{-5}$, and 3 are irreducible elements of R_5 .
 - (d) From the equation $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, show that R_5 is not a principle ideal domain.

4. Let $(R, +, \cdot)$ be a ring that contains a field F as a subring. Then R has the structure of an F -vector space, where addition is given by $+$ and scalar multiplication is performed via \cdot . Suppose that R is a finite-dimensional F -vector space. Show that if R is an integral domain, then R is a field.

5. Find the Galois group of $x^3 + 10x + 20$ over \mathbb{Q} .

6. Let p be an odd prime, and $\phi_p = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + 1 \in \mathbb{Z}[x]$. Let z be a root of ϕ_p in a splitting field over \mathbb{Q} , and let $K = \mathbb{Q}(z)$. Show there is precisely one subfield L of K such that $[K : L] = 2$. In addition, show that this L is $\mathbb{Q}(z + 1/z)$.

1. Let p be a prime number. Show that
 - (a) The center of any p -group is a p -group (that is, the center cannot be trivial),
 - (b) Any group of order p^2 must be abelian.

2. Let G be a nonabelian group of order pq , with p, q prime and $p < q$.
 - (a) Prove that p divides $q - 1$.
 - (b) Prove that the center of G is trivial.
 - (c) How many distinct conjugacy classes are there in G ?

3. The 2×2 trace-zero Hermitian matrices form a real vector space H of dimension 3. Let $SU(2) = \{g = (g_{ij})_{2 \times 2} : g_{ij} \in \mathbb{C}, {}^t \bar{g}g = g {}^t \bar{g} = I_2, \det g = 1\}$; it is the special unitary group. An element $g \in SU(2)$ acts on H by $\rho(g) : x \in H \mapsto gx {}^t \bar{g} \in H$.
 - (a) Show that there is a (positive-definite) inner product on H that is invariant under the $SU(2)$ action. (Hint: You may want to consider the determinant of the matrices in H .)
Consequently, for any $g \in SU(2)$ we have $\rho(g) \in SO(3)$, where $SO(3)$ is the special orthogonal group defined by $SO(3) = \{q = (q_{ij})_{3 \times 3} : q_{ij} \in \mathbb{R}, {}^t q q = q {}^t q = I_3, \det q = 1\}$.
 - (b) Show that $\rho : SU(2) \rightarrow SO(3)$ is a homomorphism.
 - (c) Find the kernel of $\rho : SU(2) \rightarrow SO(3)$.
 - (d) Show that $\rho : SU(2) \rightarrow SO(3)$ is surjective.

4. Prove that if R is a domain and $a \neq 0$ is not a unit in R , then $A = \langle a, x \rangle$ is not a principle ideal in $R[x]$. Explain why $\mathbb{Q}[x]$ is a Euclidean domain, but $\mathbb{Q}[x, y]$ is not.

5. Let R be a ring with identity 1 and let M be a left R -module on which 1 acts as the identity.
 - (a) Show that if $e \in R$ is in the center of R and satisfies $e^2 = e$, then we have $M = M_1 \oplus M_2$ as modules, where $M_1 = eM$ and $M_2 = (1 - e)M$. Prove that $\text{End}_R(M) \cong \text{End}_R(M_1) \oplus \text{End}_R(M_2)$ as rings.
 - (b) Now suppose $1 = e_1 + \cdots + e_n$, where e_i ($1 \leq i \leq n$) are elements in the center of R and they are orthogonal idempotents, that is, they satisfy $e_i^2 = e_i$ (for all $1 \leq i \leq n$) and $e_i e_j = 0$ (for all $1 \leq i \neq j \leq n$). State and prove a generalization of the above result.
 - (c) Let $R = \mathbb{C}[\mathbb{Z}_5]$ be the group algebra¹ of \mathbb{Z}_5 . Find a decomposition of the unit element 1 into five nonzero orthogonal idempotents. Let $M = R$, with the R -action given by the left multiplication. Show that M is isomorphic to a direct sum of five one-dimensional submodules that are pairwise nonisomorphic.

6. Let ζ be a primitive complex ninth root of unity.
 - (a) What is its minimal polynomial over \mathbb{Q} ?
 - (b) What is the degree of $\mathbb{Q}(\zeta)$ over \mathbb{Q} ?
 - (c) Find primitive elements for each field intermediate between \mathbb{Q} and $\mathbb{Q}(\zeta)$. Express them as polynomials in ζ .

¹The group algebra of a finite group G is the set $\mathbb{C}[G]$ of formal sums $\sum_{g \in G} a_g g$ ($a_g \in \mathbb{C}$) with the obvious multiplication

1. Let G be a group, G_L the group of left translates a_L ($a \in G$) of G , and $\text{Aut}(G)$ the group of automorphisms of G . The set $G_L\text{Aut}(G) = \{\sigma\tau : \sigma \in G_L, \tau \in \text{Aut}(G)\}$ is called the *holomorph* of G and is denoted $\text{Hol } G$.

- (a) Show that $\text{Hol } G$ is a group under composition and that if G is finite, then $|\text{Hol } G| = |G| \times |\text{Aut}(G)|$.
- (b) Prove that $\text{Hol}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is isomorphic to S_4 .

2. Let G be a group of order pqr where $p < q < r$ are prime. Show that G has a normal Sylow subgroup.

3. Let R be a commutative ring with identity, I_1 and I_2 ideals in R , and $\phi : R \rightarrow R/I_1 \times R/I_2$ the canonical mapping.

- (a) Describe $\ker \phi$ and show that if $I_1 + I_2 = R$ then $\ker \phi = I_1 I_2$.
- (b) Prove that when $I_1 + I_2 = R$ the mapping ϕ is surjective.
- (c) Show that $(\mathbb{Z}_{100})^\times$ is isomorphic to $(\mathbb{Z}_4)^\times \times (\mathbb{Z}_{25})^\times$.

4. Let V be a finite-dimensional vector space and let $T : V \rightarrow V$ be a linear transformation from V to itself. Define a mapping $T^* : V^* \rightarrow V^*$ by $T^*(f) = f \circ T$.

- (a) Show that T^* is a linear transformation.
- (b) Let $B = \{e_1, \dots, e_n\}$ be a basis for V and let $B^* = \{e_1^*, \dots, e_n^*\}$ be a basis for V^* . Show that the matrix for T^* relative to B^* is the transpose of the matrix for T relative to B .

5. Suppose that \mathbb{F} is a finite field and that $x^3 + ax + b \in \mathbb{F}[x]$ is irreducible. Explain why $-4a^3 - 27b^2$ must be a square in \mathbb{F} .

6. Let $g(x) = x^p - x - a \in \mathbb{Z}_p[x]$, where p is a prime and assume a is nonzero.

- (a) Show that $g(x)$ has no repeated roots in a splitting field extension.
- (b) Show that $g(x)$ has no roots in \mathbb{Z}_p .
- (c) Show that if α is a root of $g(x)$ in a splitting field extension then so is $\alpha + b$ for any $b \in \mathbb{Z}_p$.
Conclude that $\{\alpha + b : b \in \mathbb{Z}_p\}$ is a complete set of roots of $g(x)$.
- (d) Show that $g(x)$ is irreducible in $\mathbb{Z}_p[x]$.
- (e) Construct a splitting field L for $g(x)$ and determine $|\text{Gal}(L/\mathbb{Z}_p)|$.

1. Let G be a finite simple group of order n . Determine the number of normal subgroups of $G \times G$.
2. (a) State the Feit-Thompson theorem.
(b) Without using the Feit-Thompson theorem, show that there is no simple group of order $6545 = 5 \cdot 7 \cdot 11 \cdot 17$.

3. (a) Let R be a ring with ideals I, J such that $I \subseteq J$. Prove that

$$(R/I)/(J/I) \simeq R/J.$$

- (b) Give an example of a unique factorization domain that is not a principal ideal domain (PID). Prove that this ring is not a PID.
 - (c) Suppose R is a PID. Say $a, b, c \in R$ such that $\gcd(a, b) = 1 = \gcd(a, c)$. Show that $\gcd(a, bc) = 1$.
4. (a) Let F be a field, V and W finite-dimensional vector spaces over F , and $T : V \rightarrow W$ a linear transformation. Let $\{w_1, w_2, \dots, w_r\}$ be a basis for $T(V)$, and take $v_1, \dots, v_r \in V$ such that $T(v_j) = w_j$ ($1 \leq j \leq r$). Show that v_1, \dots, v_r are linearly independent. Then, let U be the space spanned by v_1, \dots, v_r , and $K = \ker T$. Prove the theorem that states $\text{rank}(T) + \text{nullity}(T) = \dim(V)$ by showing V can be realized as a **direct** sum of U and K .
(b) Let V be as above. Show that any linearly independent subset $\{v_1, \dots, v_m\}$ of V can be extended to a basis $\{v_1, \dots, v_n\}$ of V .

5. Suppose that $K[\alpha] : K$ is an extension, that α is algebraic over K , but not in K , and that β is transcendental over K . Show that $K(\alpha, \beta)$ is not a simple extension of K .

6. Let $h(x) = x^4 + 1 \in \mathbb{Q}(x)$.

- (a) Show that the four complex numbers $\pm \frac{\sqrt{2}}{2}(1 \pm i)$ are the four roots of $h(x)$ in \mathbb{C} .
- (b) Find an $\alpha \in \mathbb{C}$ such that $L = \mathbb{Q}(\alpha)$ is a splitting field extension for $h(x)$ over \mathbb{Q} .
- (c) Describe $\text{Gal}(L/\mathbb{Q})$ as a group of permutations of the roots of $h(x)$, and as a group of automorphisms of L . (The latter means: write an arbitrary $a \in L$ out in terms of a basis for L over \mathbb{Q} , and then describe what $\sigma(a)$ looks like in terms of this basis, for each $\sigma \in \text{Gal}(L/\mathbb{Q})$.)
- (d) Find all intermediate fields M between L and \mathbb{Q} ; for each such field M find a subgroup H of $\text{Gal}(L/\mathbb{Q})$ such that $M = \text{Fix}(H)$ and $H = \text{Gal}(L/M)$. Which of the extensions $M : \mathbb{Q}$ are normal?

1. (a) Suppose that G is a finite group and that there is a group homomorphism

$$h : G \longrightarrow S,$$

where S is the multiplicative group of roots of unity in the complex numbers, and which satisfies

$$(h(g))^3 = 1$$

for every element $g \in G$, but for which not every $h(g)$ has the value 1. Prove that G contains an element of order 3.

- (b) Let \mathbb{F}_7 be the finite field of 7 elements, and $GL(2, \mathbb{F}_7)$ the group of nonsingular 2×2 matrices A with entries in \mathbb{F}_7 , and multiplication of matrices as group law. Use the determinant function to construct a homomorphism

$$t : GL(2, \mathbb{F}_7) \longrightarrow S$$

which satisfies

$$(t(A))^3 = 1$$

for all $A \in GL(2, \mathbb{F}_7)$, but for which not every $t(A)$ has the value 1.

2. (a) For which prime divisors p of $n!$ are all the elements of the Sylow p -subgroups of the symmetric group S_n even permutations?
- (b) In the symmetric group S_n the conjugacy class of a particular element a (i.e., the set of elements conjugate to a) consists of all elements with the same cycle structure as a (i.e., whose decomposition as a product of disjoint cycles agrees with that of a in having the same number of cycles and of the same lengths). For what even permutations a is this also the case for the conjugacy class of a in the alternating group A_n ($n > 1$)?

3. Let A be a commutative ring with identity 1, and let M be an A -module. If there exists a chain of submodules

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_r = \{0\}$$

such that for $i = 1, \dots, r$, $M_{i-1}/M_i \simeq A/P_i$ for some maximal ideal P_i , then r is called the *length* of M and is denoted by $L_A(M)$, and M is said to have finite length.

- (a) Prove that $L_A(M)$ is well-defined.
 (b) If

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is an exact sequence of A -modules and two of the modules have finite length, then the third module also has finite length. Furthermore,

$$L_A(M) = L_A(M') + L_A(M'').$$

- (c) If

$$0 \longrightarrow M_n \longrightarrow M_{n-1} \longrightarrow \cdots \longrightarrow M_0 \longrightarrow 0$$

is an exact sequence of modules of finite length, then

$$\sum_{i=1}^n (-1)^i L_A(M_i) = 0.$$

4. An ideal \mathfrak{a} in a commutative ring R is called *primary* iff $a, b \in R$ and $ab \in \mathfrak{a}$ implies that either $a \in \mathfrak{a}$ or there is an $n \in \mathbb{N}$ such that $b^n \in \mathfrak{a}$.
- (a) Provide an example of a prime ideal in $\mathbb{C}[x, y]$.
 - (b) Let \mathfrak{a} be the ideal in $\mathbb{C}[x, y]$ generated by xy and x^2 . Prove that \mathfrak{a} is not primary.
 - (c) Prove that the radical of \mathfrak{a} , $\sqrt{\mathfrak{a}}$, is a prime ideal.
 - (d) Is $\sqrt{\mathfrak{a}}$ maximal?
5. (a) Prove that the polynomial $x^4 - 27$ is irreducible over \mathbb{Q} .
- (b) Determine a (minimal) splitting field for the polynomial $x^4 - 27$ over \mathbb{Q} . Determine the order of its Galois group (over \mathbb{Q}) and prove that it is not commutative.
6. (a) Let \mathbb{Q} denote the field of rational numbers, and let K be a (minimal) splitting field for $x^2 - 2$ over \mathbb{Q} . For what other monic irreducible polynomial in $\mathbb{Q}[x]$ is K a splitting field?
- (b) Let L be a (minimal) splitting field for $x^3 + x + 1$ over \mathbb{F}_2 , the field of 2 elements. Find all other irreducible polynomials in $\mathbb{F}_2[x]$ for which L is a splitting field over \mathbb{F}_2 .

1. Let G be a finite group and N a normal subgroup. Show that
 - (a) The intersection with N of a Sylow p -subgroup of G is a Sylow p -subgroup of N and every Sylow p -subgroup of N is obtained in this way.
 - (b) The image in G/N of a Sylow p -subgroup of G is a Sylow p -subgroup of G/N and every Sylow p -subgroup of G/N is obtained in this way.

2. Let G and H be groups and $\theta : H \rightarrow \text{Aut}(G)$ a homomorphism. Let $G \times_{\theta} H$ be the set $G \times H$ with the following binary operation: $(g, h)(g', h') = (g[\theta(h)(g')], hh')$.
 - (a) Show that $G \times_{\theta} H$ is a group with the identity element (e, e') and $(g, h)^{-1} = (\theta(h^{-1})(g^{-1}), h^{-1})$. (You may assume without proving it that the operation is associative.)
 - (b) Use the construction of (a), with G a cyclic group of order 7, to show that there is a group K with 105 elements generated by elements a, b, c such that $a^5 = e, b^3 = e, c^7 = e, ab = ba, bc = cb, ac = c^4a$.
 - (c) In the group described in (b), determine the number of Sylow subgroups.

3. (a) Suppose $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ is a short exact sequence of abelian groups. Show that $\text{rank } A$ is finite if and only if $\text{rank } A'$ and $\text{rank } A''$ are finite. If so, show that $\text{rank } A = \text{rank } A' + \text{rank } A''$.
 - (b) Suppose $0 \rightarrow C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} \cdots \rightarrow C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0 \rightarrow 0$ is a chain of abelian groups, i.e., C_i is an abelian group and $d_i : C_i \rightarrow C_{i-1}$ is a homomorphism such that $d_{i-1} \circ d_i = 0$, for each i . Let $H_i = \frac{\ker d_i}{\text{Im } d_{i+1}}$ ($i = 0, 1, \dots, n$). Assume that $\text{rank } C_i$ is finite, for all i . Define two polynomials

$$m(t) = \sum_{i=0}^n \text{rank } C_i t^i, \quad p(t) = \sum_{i=1}^n \text{rank } H_i t^i.$$
 Show that there is a polynomial $q(t)$ with nonnegative coefficients such that $m(t) = p(t) + (1+t)q(t)$.

4. Let R be a commutative ring and M be a module over R . A submodule N is a *characteristic* submodule if $\varphi(N) \subset N$ for any R -endomorphism φ of M . Show that
 - (a) $\forall r \in R, rM$ and $\text{Ann}(r) = \{m \in M : rm = 0\}$ are characteristic submodules of M .
 - (b) If N is a characteristic submodule of M , and P, Q are complementary submodules of M , i.e., $P \oplus Q = M$, then $N \cap P, N \cap Q$ are complementary submodules of N .

5. (a) Suppose H is a subgroup of S_n ($n \geq 2$) which contains both an n -cycle and a transposition. Show that $H = S_n$.
 - (b) Show that the roots of the polynomial $P(x) = x^5 - 6x + 3$ cannot be expressed by radicals.

6. Let K be a field of characteristic 0, and let $K(x)$ be a simple transcendental extension. Let G be the subgroup of the group of K -automorphisms of $K(x)$ generated by an automorphism that takes x to $x + 1$. Show that K is the fixed field of G .

1. Determine the Galois groups of the following polynomials in $\mathbb{Q}[x]$:
 - (a) $x^4 - 7x + 10$.
 - (b) $x^3 - 2$.
 - (c) $x^5 - 9x + 3$.

2. (a) If G is a group of order $5^3 \cdot 7 \cdot 17$ show that G has normal subgroups of sizes 5^3 , $5^3 \cdot 7$, and $5^3 \cdot 17$.
(b) Show that there is a nonabelian nilpotent group of order $5^3 \cdot 7 \cdot 17$. [Hint: To construct a nonabelian group of order 5^3 , work in S_{25} to find nonidentity elements a, b such that a is of order 25, b is of order 5, and $b^{-1}ab = a^6$. A finite group is nilpotent if it is the direct product of its Sylow subgroups.]

3. Let R be a ring with 1. An element x in R is called *nilpotent* if $x^m = 0$ for some positive integer m .
 - (a) Show that if $n = a^k b$ for some integers a and b then the coset \overline{ab} is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.
 - (b) If $a \in \mathbb{Z}$ is an integer, show that the element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a . In particular, determine the nilpotent elements of $\mathbb{Z}/36\mathbb{Z}$ explicitly.
 - (c) If R is any commutative ring with 1 and x is a nilpotent element, show that $1 + x$ is a unit for R (i.e., is invertible). [Hint: As motivation, think of the sum of the geometric series.]

4. Let R be a ring with 1 and M a left unitary R -module. An element m in M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted $\text{Tor}(M) = \{m \in M : rm = 0 \text{ for some nonzero } r \in R\}$.
 - (a) Prove that if R is an integral domain then $\text{Tor}(M)$ is a submodule of M (called the torsion submodule of M).
 - (b) Give an example of a ring R and an R -module M such that $\text{Tor}(M)$ is not a submodule. [Hint: Consider letting R be itself a left R -module where R is some ring which is not an integral domain.]
 - (c) Show that if R has zero divisors then every nonzero R -module has nonzero torsion elements.

5. Give a representative element of each conjugacy class of the elements of the alternating group A_5 , and determine the number of elements in its class.

6. (a) Prove that $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over \mathbb{Z}_2 .
(b) What are the other irreducible quartic polynomials over \mathbb{Z}_2 ?
(c) If θ is one of the roots of $f(x)$, what are the others (expressed as polynomials in θ of least possible degree)?
(d) Give a method for finding an element φ (expressed as a polynomial in θ) of the splitting field $\mathbb{Z}_2(\theta)$ such that $[\mathbb{Z}_2(\varphi) : \mathbb{Z}_2] = 2$.

1. Let G be a finite group, and C be the center of G .
 - (a) Show that the index $[G : C]$ is not a prime number.
 - (b) Give an example where $[G : C] = 4$.
2. Let G be a finite group that acts transitively on a set S . Recall that G is said to act *doubly transitively* if for every pair $(a, b), (c, d)$ there is a $g \in G$ such that $g(a) = c$ and $g(b) = d$.
In (a) and (b) below, assume that G is a finite group that acts transitively on a set S . Let s be in S , and let

$$H = \{g \in G : g(s) = s\}$$

be its isotropy group. Note then H acts on the complement $S - \{s\}$.

- (a) Show that G acts doubly transitively on S if and only if H acts transitively on $S - \{s\}$.
 - (b) Suppose there is a subgroup T of G of order two, T not contained in H , such that $G = HTH$. Show that G acts doubly transitively on S .
3. Let R be a commutative ring with identity. Suppose that for some $a, b \in R$, the ideal $Ra + Rb$ is principal. Prove that the ideal $Ra \cap Rb$ is principal.

4. Let S be a commutative ring with identity, $R = S[x_1, \dots, x_n]$. Let I be the ideal of R generated by the quadratic monomials $\{x_i x_j : 1 \leq i, j \leq n\}$, and ϕ the natural projection

$$\phi : R \rightarrow R/I.$$

- (a) Show that R/I is a free S -module and find its rank.
- (b) For $f \in R$ define $f' \in R/I$ by $f' = \phi(f) - \phi(f(0, \dots, 0))$. Show that

$$(fg)' = \phi(f)g' + \phi(g)f'.$$

- (c) Show that for all positive integers n , $(f^n)' = n\phi(f)^{n-1}f'$.

5. Determine the Galois group (using generators and relations if you would like) over K of $x^5 - 3$ when:

- (a) $K = \mathbb{Q}$.
- (b) $K = \mathbb{F}_{11}$, the finite field with 11 elements.

6. We call a six degree polynomial *symmetric* if $x^6 f(1/x) = f(x)$. Let f be a symmetric six degree polynomial in $\mathbb{Q}[x]$.

- (a) Suppose r is a root of f in a splitting field of f . Show that $[\mathbb{Q}(r + 1/r) : \mathbb{Q}] \leq 3$.
- (b) Deduce from (a) that the Galois group of f is solvable. [Hint: All groups of order less than 60 are solvable.]

1. (a) Show that there is no simple nonabelian group of order 76.
 (b) Show that there is no simple nonabelian group of order 80.

2. Let p be an odd prime. Show that a group of order $2p$ is either cyclic, or is isomorphic to the dihedral group D_{2p} . (Recall that the dihedral group D_n is the group of symmetries of a regular n -gon in a plane.)

3. Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$, where $\sqrt{-3}$ is a root of $x^2 + 3$ in some splitting field. Let

$$\begin{aligned} S &= \mathbb{Z} \left[\frac{1 + \sqrt{-3}}{2} \right] \\ &= \left\{ a + b \left(\frac{1 + \sqrt{-3}}{2} \right) : a, b \in \mathbb{Z} \right\}. \end{aligned}$$

(a) Show that S is a Euclidean domain with respect to the norm

$$\delta \left(a + b \left(\frac{1 + \sqrt{-3}}{2} \right) \right) = a^2 + ab + b^2.$$

(b) Show that R is not a Euclidean domain with respect to the norm

$$\delta(a + b\sqrt{-3}) = a^2 + 3b^2.$$

[Hint: Is R a unique factorization domain?]

4. Let F be a field and let t be transcendental over F . Recall that if $P(t)$ and $Q(t)$ are nonzero relatively prime polynomials in $F[t]$, which are not both constant, then

$$[F(t) : F(P(t)/Q(t))] = \max\{\deg P, \deg Q\},$$

a fact you may use, if needed.

(a) Prove that $\text{Aut}(F(t)/F) \cong GL_2(F)/\{\lambda I : \lambda \in F^\times\}$, where

$$GL_2(F) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in F \text{ and } ad - bc \neq 0 \right\} \quad \text{and} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(b) Let \mathbb{F}_2 be the field with two elements. Show that $\text{Aut}(\mathbb{F}_2(t)/\mathbb{F}_2) \cong S_3$.

(c) Find the subfields of $\mathbb{F}_2(t)$ which are the fixed fields of the subgroups of $\text{Aut}(\mathbb{F}_2(t)/\mathbb{F}_2)$.

5. Show that $f(x) = 2x^5 - 10x + 5$ is not solvable by radicals over the rational numbers.

6. An *ultrafilter* on $\mathbb{N} = \{0, 1, 2, \dots\}$ is a collection U of subsets of \mathbb{N} such that the following conditions hold:

- (i) $\mathbb{N} \in U$.
- (ii) $\emptyset \notin U$.
- (iii) If $x \in U$ and $x \subseteq y \subseteq \mathbb{N}$, then $y \in U$.
- (iv) If $x, y \in U$, then $x \cap y \in U$.
- (v) For any $x \subseteq \mathbb{N}$, $x \in U$ or $\mathbb{N} - x \in U$. ($\mathbb{N} - x$ is the complement of x in \mathbb{N} .)

Suppose that $\langle F_i : i \in \mathbb{N} \rangle$ is a system of fields, and U is an ultrafilter on \mathbb{N} . Consider the full direct product $\prod_{i \in \mathbb{N}} F_i$, which is a commutative ring with identity, consisting of all functions a with domain \mathbb{N} , with $a_i = a(i) \in F_i$ for all i , the ring operations being coordinate-wise. Let $I = \{a \in \prod_{i \in \mathbb{N}} F_i : \{i \in \mathbb{N} : a_i = 0\} \in U\}$.

- (a) Show that I is a maximal ideal of $\prod_{i \in \mathbb{N}} F_i$.
- (b) Suppose that for each $i \in \mathbb{N}$, every polynomial in $F_i[x]$ of positive degree at most i has a root in F_i . Suppose that $\mathbb{N} - F \in U$ for every finite subset F of \mathbb{N} . Show that $\prod_{i \in \mathbb{N}} F_i / I$ is an algebraically closed field.

1. Let G be a group of order $429 = 3 \cdot 11 \cdot 13$.
 - (a) Show that every subgroup of order 13 in G is normal in G . (Use the Sylow theorems.)
 - (b) Show that every subgroup of order 11 in G is normal in G .
 - (c) Classify (up to isomorphism) all groups of order 429.

2. Let \mathbb{Q} denote the field of rational numbers and let $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.
 - (a) Find the Galois group of K over \mathbb{Q} and show that K is a Galois extension of \mathbb{Q} . Express all of the elements of the Galois group as permutations of the roots of $(x^2 - 5)(x^2 - 7)$.
 - (b) Find all the subfields of K and match them up with the subgroups of the Galois group as is indicated by the Fundamental Theorem of Galois Theory.

3. Let $K = GF(p^m)$ be the finite field with $q = p^m$ elements (p is a rational prime number). Let V be an n -dimensional vector space over K . Give explicit formulas for the following numbers:
 - (a) The number of elements of V .
 - (b) The number of distinct bases of V . Give it for both ordered and unordered bases.
 - (c) The order of the general linear group $GL_n(K)$.
 - (d) Let $K = GF(3)$ be the field with 3 elements. Verify that there are 48 nonsingular 2×2 matrices over K . Also show that the only nonsingular 2×2 matrix A over K that satisfies the equation $A^5 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ is the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ itself.

4. Let V be an n -dimensional vector space over an arbitrary field K and let $f : V \rightarrow V$ be a linear transformation. Show that there exists a basis for V such that the matrix representation for f with respect to that basis is diagonal if and only if the minimal polynomial for f is a product of distinct linear factors.

5. Let Z_n denote the cyclic group of order n . Let $G = Z_{81} \oplus Z_{30} \oplus Z_{16} \oplus Z_{45}$.
 - (a) What is the largest cyclic subgroup of G ? Give a generator for this group in terms of the generators for the cyclic components of G . Please denote the generators for the groups Z_{81} , Z_{30} , Z_{16} , and Z_{45} by a, b, c and d , respectively.
 - (b) How many elements of order three does G have?
 - (c) How many elements of order nine does G have?

6. Recall that a Euclidean domain is an integral domain R together with a natural number valued function N defined on the nonzero elements of R which has the property that, given a and b in R with b nonzero, we can find q and r in R such that $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$. Now let $R = \mathbb{Z}[\sqrt{-2}] = \{m + n\sqrt{-2} : m, n \in \mathbb{Z}\}$, where \mathbb{Z} is the ring of rational integers. Let $N(m + n\sqrt{-2}) = m^2 + 2n^2$.
 - (a) Show that R is a Euclidean domain.
 - (b) Decide whether $x^3 + 2\sqrt{-2}x + 4$ is irreducible in $\mathbb{Q}(x)$, where \mathbb{Q} is the field of rational numbers.

7. Let $R = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ and let $N\left(m + n\frac{1+\sqrt{-7}}{2}\right) = \frac{(2m+n)^2 + 7n^2}{4}$, where \mathbb{Z} is the ring of rational integers and $m, n \in \mathbb{Z}$. Show that R is a Euclidean domain. (Your proof should also work if -7 is replaced by -11 and $N\left(m + n\frac{1+\sqrt{-11}}{2}\right) = \frac{(2m+n)^2 + 11n^2}{4}$.)

1. Suppose the group G has a nontrivial subgroup H which is contained in every nontrivial subgroup of G . Prove that H is contained in the center of G .

2. Let n be an odd positive integer, and denote by S_n the group of all permutations of $\{1, 2, 3, \dots, n\}$. Suppose that G is a subgroup of S_n of 2-power order. Prove that there exists $i \in \{1, 2, 3, \dots, n\}$ such that for all $\sigma \in G$ one has $\sigma(i) = i$.

3. Let p be an odd prime and \mathbb{F}_p the field of p elements. How many elements of \mathbb{F}_p have square roots in \mathbb{F}_p ? How many have cube roots in \mathbb{F}_p ? Explain your answers.

4. Suppose that $W \subseteq V$ are vector spaces over a field with finite dimensions m and n (respectively). Let $T : V \rightarrow V$ be a linear transformation with $T(V) \subseteq W$. Denote the restriction of T to W by T_W . Identifying T and T_W with matrices, prove that $\det(I_n - xT) = \det(I_m - xT_W)$ where x is an indeterminate and I_m, I_n denote the $m \times m, n \times n$ identity matrices.

5. Let \mathbb{Q} be the field of rational numbers. For θ a real number, let $F_\theta = \mathbb{Q}(\sin \theta)$ and $E_\theta = \mathbb{Q}(\sin \frac{\theta}{3})$. Show that E_θ is an extension field of F_θ , and determine all possibilities for $\dim_{F_\theta} E_\theta$.

6. Let $g(x) = x^7 - 1 \in \mathbb{Q}[x]$, and let K be a splitting field for $g(x)$ over \mathbb{Q} .

(a) Show that $g(x) = (x - 1)h(x)$ where $h(x)$ is irreducible in $\mathbb{Q}[x]$. (Hint: Study $h(x + 1)$ by first writing $h(x) = g(x)/(x - 1)$. Use Eisenstein's criterion to show $h(x + 1)$ is irreducible.)

(b) Show that $G = \text{Gal}(K/\mathbb{Q})$ is cyclic of order 6, and has as a generator the map that takes $\omega \mapsto \omega^3$ for any root ω of $g(x)$.

(c) Let ω be a complex 7th root of 1. Let

$$x_1 = \omega + \omega^2 + \omega^4, \quad x_2 = \omega + \omega^6.$$

Find subgroups H_1, H_2 of G such that $\mathbb{Q}(x_1)$ is the fixed field of H_1 and $\mathbb{Q}(x_2)$ is the fixed field of H_2 . Find $[\mathbb{Q}(x_1) : \mathbb{Q}]$ and $[\mathbb{Q}(x_2) : \mathbb{Q}]$.

(d) Show that $\mathbb{Q}(x_1)$ and $\mathbb{Q}(x_2)$ are the only fields M with $\mathbb{Q} \subset M \subset \mathbb{Q}(\omega)$. (Here \subset denotes proper containment.)

1. Suppose $p > q$ are prime numbers and that q does not divide $p - 1$. Show that every group G of order pq is cyclic.
2. Let R be a ring with multiplicative identity 1. An element $r \in R$ is called *nilpotent* if $r^n = 0$ for some positive integer $n > 0$. Let N denote the set of nilpotents in R .
 - (a) Show that if R is commutative then N is an ideal. Give an example of a noncommutative R for which N is not an ideal.
 - (b) An ideal I in a commutative ring is called *primary* if for every $xy \in I$, either $x \in I$ or $y^m \in I$ for some positive integer m . Suppose that R is commutative and that I is an ideal in R . Show that I is primary if and only if every zero divisor in R/I is nilpotent.
3. Consider the set of numbers $R = \left\{ a + b \left(\frac{1 + \sqrt{-15}}{2} \right) : a, b \in \mathbb{Z} \right\} \subset \mathbb{Q}(\sqrt{-15})$.
 - (a) Show that R is a ring, and that the automorphism $\sqrt{-15} \mapsto -\sqrt{-15}$ of $\mathbb{Q}(\sqrt{-15})$ induces an automorphism of R .
 - (b) What is the norm of $a + b \left(\frac{1 + \sqrt{-15}}{2} \right)$ for integers a, b ?
 - (c) Find all the units in R .
 - (d) Find all factorizations of 4 into irreducibles in R .
 - (e) Give an example in R of an irreducible which isn't prime.
4. Let ζ be a primitive 12^{th} root of unity.
 - (a) Find the Galois group of $\mathbb{Q}(\zeta)$ over \mathbb{Q} .
 - (b) Let $\Phi_n(x)$ denote the n^{th} cyclotomic polynomial over \mathbb{Q} . What is the degree of $\Phi_{24}(x)$ over \mathbb{Q} ?
 - (c) When $\Phi_{24}(x)$ is factored over $\mathbb{Q}(\zeta)$, how many factors are there, and what are their degrees?
5. Let q be a power of a prime, and r a positive integer. Let \mathbb{F}_q and \mathbb{F}_{q^r} denote, respectively, the fields with q and q^r elements. Let G denote the Galois group of \mathbb{F}_{q^r} over \mathbb{F}_q , and let N denote the norm map, $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$ from \mathbb{F}_{q^r} to \mathbb{F}_q . Show that

$$N : \mathbb{F}_{q^r}^\times \rightarrow \mathbb{F}_q^\times$$
 is a surjective homomorphism.
6. Let G be a finite group of order n , and suppose for each prime p dividing n there is a unique Sylow p -subgroup. Show that G is solvable. (Be sure to carefully state any theorems about solvable groups that you use.)

1. Let G be a group, G_L the group of left translates a_L ($a \in G$) of G (that is, for $a \in G$, $a_L : G \rightarrow G$ is defined by $a_L(g) = ag$).

- Show that $G_L \text{Aut}(G)$ (that is, the set $\{xy : x \in G_L, y \in \text{Aut}(G)\}$) is a group of transformations of G . $G_L \text{Aut}(G)$ is called the *holomorph* of G and is denoted $\text{Hol}(G)$.
- Show $G_R \subset \text{Hol}(G)$, where G_R is the group of right translates of G .
- Show that if G is finite, then $|\text{Hol}(G)| = |G| |\text{Aut}(G)|$.

2. Let $h(x) = x^4 + 1 \in \mathbb{Q}[x]$, and let $L \subset \mathbb{C}$ be a splitting field for $h(x)$ over \mathbb{Q} .

- Find the four roots of $h(x)$ in \mathbb{C} .
- Find an $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$.
- Describe all elements of $G = \text{Gal}(L/\mathbb{Q})$ as permutations of the roots of $h(x)$.
- Find all intermediate fields M between L and \mathbb{Q} ; for each such field M find a subgroup H of G such that M is the fixed field of H and $H = \text{Gal}(L/M)$. Which of the extensions M are normal over \mathbb{Q} ?

3. Let R be a ring with identity and M an R -module.

- Show that, if $m \in M$, then $\{x \in R : xm = 0\}$ is a left ideal of R .
- Let A be a left ideal of R , and $m \in M$. Show that $\{xm : x \in A\}$ is a submodule of M .
- Suppose that M is *irreducible*, which means that M has no submodules other than (0) and M . Let $m_0 \in M$, $m_0 \neq 0$. Show that $A = \{x \in R : xm_0 = 0\}$ is a maximal left ideal in R .

4. Let $g(x) = x^p - x - a \in \mathbb{Z}/p\mathbb{Z}[x]$, where $p \in \mathbb{Z}$ is a prime, and a a nonzero element of $\mathbb{Z}/p\mathbb{Z}$.

- Show that $g(x)$ has no repeated roots in a splitting field extension.
- Show that $g(x)$ has no roots in $\mathbb{Z}/p\mathbb{Z}$.
- Show that, if c is a root of $g(x)$ in a splitting field extension, then so is $c+i$ for any $i \in \mathbb{Z}/p\mathbb{Z}$. Conclude that $\{c+i : i \in \mathbb{Z}/p\mathbb{Z}\}$ is a complete set of roots of $g(x)$.
- Show that $g(x)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$.
- Construct a splitting field extension L for $g(x)$ over $\mathbb{Z}/p\mathbb{Z}$.
- Find the Galois group $\text{Gal}(L/(\mathbb{Z}/p\mathbb{Z}))$. Describe this group as a group of permutations of the roots of $g(x)$.

5. Let N be a positive integer, and let L_N denote the set of functions $f : \mathbb{Z} \rightarrow \mathbb{C}$ such that $f(t) = f(t+N)$ for all $t \in \mathbb{Z}$. Define the *convolution* $f * g$ of functions $f, g \in L_N$ by

$$f * g(t) = \frac{1}{N} \sum_{0 \leq y \leq N-1} f(t-y)g(y) \quad (t \in \mathbb{Z}).$$

- Show that, under the usual addition of functions and the above convolution of functions, L_N is a commutative ring, which identity δ_N given by

$$\delta_N(x) = \begin{cases} N & \text{if } N|x, \\ 0 & \text{if not.} \end{cases}$$

You may assume (that is, you needn't prove) that L_N is an abelian group under addition.

5. (b) Suppose $M|N$ for some positive integer M , and define

$$\delta_M(x) = \begin{cases} M & \text{if } M|x, \\ 0 & \text{if not.} \end{cases}$$

Show that δ_M is an *idempotent* element of L_N : that is, $\delta_M * \delta_M = \delta_M$.

- (c) Let M, N be as above, and let $f, g \in L_M$, so that also $f, g \in L_N$. Suppose, for clarity, we denote the convolution in L_M by $*'$. Show that $f * g = f *' g$, where $*$ again denotes the convolution in L_N .
- (d) Show that, for M and N as above, the map $f \rightarrow f * \delta_M$ is a ring homomorphism of $(L_N, +, *, 0, \delta_N)$ onto $(L_M, +, *', 0, \delta_M)$.
6. Let H and K be subgroups of a group G .
- (a) Show that the set of maps $\{x \rightarrow hxk : h \in H, k \in K\}$ is a group of transformations of the group G .
- (b) Let HxK denote the orbit of x relative to the above group of transformations of G . Show that if G is finite then $|HxK| = |H| |K : x^{-1}Hx \cap K| = |K| |H : x^{-1}Kx \cap H|$.

1. Let G be a group of order $3 \times 11 \times 17 = 561$. Let H be a group of order $11 \times 17 = 187$.
 - (a) Prove that H is abelian and cyclic. [Hint: Use Sylow theorems.]
 - (b) Prove that the Sylow 11- and Sylow 17-subgroups of G are both normal in G .
 - (c) Is G necessarily abelian? If “yes,” prove it; if “no,” give an example of a nonabelian group of order 561. Are all abelian groups of order 561 cyclic?

2. Let Z_n denote the cyclic group of order n . Let $G = Z_9 \oplus Z_{27} \oplus Z_{25} \oplus Z_5 \oplus Z_{35}$; let $Z_9 = \langle a \rangle$; $Z_{27} = \langle b \rangle$; $Z_{25} = \langle c \rangle$; $Z_5 = \langle d \rangle$; $Z_{35} = \langle e \rangle$; i.e., a, b, c, d, e are generators for the summands of G .
 - (a) What is the largest cyclic subgroup of G ? Give a generator of that subgroup in terms of a, b, c, d, e . You do not need to justify your answer.
 - (b) How many elements of order 5 does G have? Justify your answer.
 - (c) How many elements of order 25 does G have? Justify your answer.

3. (a) Let F be a field and $F[x]$ the ring of polynomials in one indeterminate over F . Note that $F[x]$ is an integral domain.
 - (i) Is $F[x]$ a Euclidean domain?
 - (ii) Is $F[x]$ a principal ideal domain?
 - (iii) Is $F[x]$ a unique factorization domain?
 - (iv) Are all its nonzero prime ideals maximal?
(Explain your answers. You may quote relevant theorems. In some cases, counterexamples may be appropriate.)(b) Answer the same questions ((i)-(iv)) for the integral domain $F[x, y]$, the ring of polynomials in two indeterminates over F . Again, explain your answers.

4. Let R be a commutative ring. An R -module M is said to be *cyclic* if it is generated by one of its elements.
 - (a) Show that every nonzero cyclic R -module M is isomorphic to R/J , where J is an ideal of R .
 - (b) Show that if R is a principal ideal domain, then every submodule of a cyclic R -module is again cyclic.

5. Let p be a prime number. Let \mathbb{F}_p denote the field $\mathbb{Z}/p\mathbb{Z}$.
 - (a) Suppose that K is an extension of \mathbb{F}_p of degree n . Show that K is the splitting field for $f(x) = x^{p^n} - x$.
 - (b) Prove that the Galois group of K (in part (a)) over \mathbb{F}_p is cyclic.
 - (c) Let \mathbb{F}_{p^m} denote a field with p^m elements. Show that \mathbb{F}_{p^m} contains a subfield \mathbb{F}_{p^n} of p^n elements if and only if n divides m .

6. (a) Suppose that a and b are complex numbers and that K is a subfield of the complex numbers such that $[K(a) : K] = 2$ and $[K(b) : K] = 3$. Suppose that $K(b)$ is a normal extension of K . Prove that $K(a, b)$ is a normal extension of K and that $K(a + b) = K(a, b)$.
(b) Suppose that K and b are as in (a), except that $K(b)$ is not a normal extension of K (but still $[K(b) : K] = 3$). Let L be an extension of $K(b)$ which is a splitting field for the minimal polynomial of b over K . Show that there exists an element a in L such that $[K(a) : K] = 2$. Show that $L = K(a, b)$. Let b' be another zero of the minimal polynomial for b over K . Show that $K(b + b') \neq L$, but that $K(b - b') = L$.

1. Let G be a finite group. A *character* on G is a homomorphism $\chi : G \rightarrow \mathbb{C}^*$ taking its values in the multiplicative group of the complex numbers. Let \widehat{G} denote the set of all characters on G . Show:

- If χ_1 and χ_2 are in \widehat{G} , then the definition $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$ for all g in G makes \widehat{G} into a group.
- If χ and g are in \widehat{G} and G , respectively, then $\chi(g)$ is a root of unity.
- For any x in \widehat{G} , $G/\ker(\chi)$ is cyclic.
- If χ is in \widehat{G} , then $\sum \chi(g)$, where the sum is taken over the elements of G , is either $n = [G : 1]$ or 0 depending on whether χ is the identity element of \widehat{G} or not.

2. Let p be a rational prime and let k be a field with $q = p^n$ elements. Let $M_2(k)$ denote the ring of 2×2 matrices over k , and $GL_2(k)$ the subset of $M_2(k)$ consisting of matrices with nonzero determinant.

- Show $GL_2(k)$ is a group under matrix multiplication.
- Show that order of $GL_2(k)$ is $r = (q^2 - q)(q^2 - 1)$.
- Show that for any matrix $A \in M_2(k)$,

$$A^{r+2} = A^2.$$

[Hint: Part (c) can be done using part (b) or by using the Theory of Canonical Forms.]

3. A field K is called *formally real* if the conditions $x_i \in K$ and $\sum_{i=1}^n x_i^2 = 0$ for some $n > 0$ imply that each x_i vanishes. It is called *real, closed* if it is formally real and no proper algebraic extension is formally real.

- Show that K is formally real if and only if -1 cannot be expressed as a sum of squares in K .
- Show that if K is real, closed then every sum of squares in K is a square in K .
- Let K be real, closed and let $P = \{\text{all nonzero finite sums of squares in } K\}$. Show that P satisfies the following properties: (i) If a and b are in P , then so are ab and $a + b$. (ii) For any a in K , exactly one of the following holds: $a = 0$, a is in P or $-a$ is in P .

4. Let ω_1 and ω_2 be a pair of complex numbers which are linearly independent over the reals. Let $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be the (necessarily free) abelian group generated by these complex numbers. Clearly $nL \subseteq L$ for any integer n . Let $R = \{z \in \mathbb{C} : zL \subseteq L\}$ and suppose R contains a non-integer z . Show:

- $\tau = \omega_1/\omega_2$ generates a quadratic extension of the rational numbers.
- If the minimal polynomial for τ is of the form $\tau^2 - r\tau - s$ for suitable integers r and s , then $R = \mathbb{Z}[\tau]$.

5. Let ω be a primitive 10^{th} root of unity in \mathbb{C} .
- (a) Find the Galois group of $\mathbb{Q}(\omega)$ over \mathbb{Q} (where \mathbb{Q} is the field of rational numbers).
 - (b) Let Φ_n denote the n^{th} cyclotomic polynomial over \mathbb{Q} . What is the degree of Φ_{20} over \mathbb{Q} ?
 - (c) Using the notation of parts (a) and (b), determine how many factors there are and what their degrees are when Φ_{20} is factored into irreducible factors over $\mathbb{Q}(\omega)$.
6. Let C_2 be the set of Sylow 2-subgroups of the symmetric group S_5 , and let C_3 be the set of Sylow 3-subgroups.
- (a) What are the cardinalities of C_2 and C_3 ?
 - (b) Let $G_2 \in C_2$ and $G_3 \in C_3$. Describe G_2 and G_3 in terms of a faithful action on a set of 5 symbols. (In the case of the Sylow 2-groups, look at the symmetries of a labelled square.)

1. Let G be a simple group of order 60. Determine how many elements of order 3 G must have. (Do not assume that you already know that $G \simeq A_5$).

2. Let the vertices of a regular n -sided polygon ($n \geq 3$) be labelled consecutively from 1 to n , i.e., with vertices $i, i+1$ endpoints of one side of the polygon. The only symmetries are rotations $\varphi_j \in S_n$ ($j = 1, \dots, n$) where $\varphi_j(i) = j + i$ and reflections $\psi_j \in S_n$ ($j = 1, \dots, n$) where $\psi_j(i) = j - i$. (The addition and subtraction in these definitions are modulo n .) Let Γ be the subgroup of S_n generated by φ_j, ψ_j ($j = 1, \dots, n$).

(a) Show that $\{\varphi_1, \psi_1\}$ generate Γ .

(b) Show that Γ is dihedral, i.e., isomorphic to D_n , the group generated by a, b subject to the relations $a^n = b^2 = e, bab^{-1} = a^{-1}$.

(c) (i) For which n are all φ_j 's and ψ_j 's even permutations of $\{1, \dots, n\}$? (ii) For which n are all φ_j 's even permutations and all ψ_j 's odd ones? (iii) For the remaining n , which φ_j 's and ψ_j 's are even?

3. Consider the polynomial ring $R = \mathbb{Z}[x]$. Consider the ideals

$$I = (x), \quad J = (5, x), \quad K = (2x, x^2 + 1).$$

Which of these are prime ideals? Which are maximal ideals? Give explanations!

4. Let R be a principal ideal domain and M an R -module that is annihilated by the nonzero proper ideal (a) . Let $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the (unique) factorization of a into distinct prime powers in R . Let $M_i = \{m \in M : p_i^{\alpha_i} m = 0\}$. Show that $M_1 + \cdots + M_k$ is in fact a direct sum and that $M = M_1 \oplus \cdots \oplus M_k$.

5. Let K_1, K_2, K_3, K_4 denote splitting fields for $x^3 - 2$ over \mathbb{Q} , $(x^3 - 2)(x^2 + 3)$ over \mathbb{Q} , $x^9 - 1$ over \mathbb{Q} and $x^{64} - x$ over \mathbb{Z}_2 , respectively. Consider the Galois groups $\text{Gal}(K_1/\mathbb{Q})$, $\text{Gal}(K_2/\mathbb{Q})$, $\text{Gal}(K_3/\mathbb{Q})$ and $\text{Gal}(K_4/\mathbb{Z}_2)$.

(a) Which of these groups are isomorphic?

(b) If ζ is a primitive 9th root of unity (over \mathbb{Q}), find an element $\alpha \notin \mathbb{Q}$ expressed as a polynomial in ζ such that the field $\mathbb{Q}(\alpha) \neq K_3$.

6. (a) Let $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ be of degree 3 and irreducible over \mathbb{Q} . In its splitting field K , $f(x) = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Show that $[K : \mathbb{Q}] = 3$ or $[K : \mathbb{Q}] = 6$ when $(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$ does or does not lie in \mathbb{Q} , respectively.

(b) Determine the degree $[L : \mathbb{F}_3]$ where \mathbb{F}_3 is the field with 3 elements and L is the splitting field (over \mathbb{F}_3) of $x^3 - x + 1$.

1. Let G be a group. If U and V are subgroups of G , we let $U \vee V$ denote the smallest subgroup of G containing $U \cup V$.

- (a) Suppose that H, K , and L are normal subgroups of G . Show: If $H \subseteq L$, then $H \vee (K \cap L) = (H \vee K) \cap L$.
- (b) Give an example showing that part (a) does not work for arbitrary subgroups (i.e., if the subgroups are not assumed to be normal). [Hint: Look at subgroups of A_4 .]

2. (a) Let G be a group, Z its center. Prove that if the factor group G/Z is cyclic, then G is abelian.

- (b) Let p be a prime and let P be a nonabelian group of order p^3 . Prove that the center Z of P is a cyclic group of order p , and the factor group P/Z is the direct product of two cyclic groups of order p . [Note: You may use without proof standard results about finite p -groups.]

3. Let R be a ring with unit element 1. Using its elements we define a ring R' by defining

$$c \oplus d = c + d + 1 \text{ and}$$

$$c * d = cd + c + d \text{ for all elements } c, d \text{ in } R \text{ (where the addition and multiplication of the right hand side of these relations are those of } R \text{).}$$

- (a) Prove that R' is a ring under the operations \oplus and $*$.
- (b) Which element is the zero element of R' ?
- (c) Which element is the unit element of R' ?
- (d) Prove that R is isomorphic to R' .

4. Let A be a commutative ring satisfying the ascending chain condition for ideals. Let $\phi : A \rightarrow A$ be a ring homomorphism of A onto itself. Prove that ϕ is an automorphism. [Hint: Consider the powers ϕ^n .]

5. (a) Let K be the splitting field of $x^4 - 2$ over the field of rationals \mathbb{Q} . Find two subfields E_1 and E_2 of K such that $[K : E_1] = [K : E_2] = 2$ but E_1 and E_2 are not isomorphic.

- (b) Let K be the splitting field of $x^7 - 3x^3 - 6x^2 + 3$ over \mathbb{Q} and let E_1 and E_2 be any subfields of K such that $[K : E_1] = [K : E_2] = 7$. Prove that E_1 and E_2 are isomorphic. [Hint: Use the Fundamental Theorem of Galois Theory.]

6. (a) Determine the splitting field K of the polynomial $x^{12} - 1$ over the field of rational numbers \mathbb{Q} . Give generators for K over \mathbb{Q} and find the degree $[K : \mathbb{Q}]$.

- (b) Prove that for all positive integers n , $\cos(2\pi/n)$ is an algebraic number.

ALGEBRA PRELIM

JANUARY 1993

DO ALL THREE QUESTIONS IN PART A. DO ANY THREE OF THE FOUR QUESTIONS IN PART B.

PART A

1. Let A be an associative ring with identity 1. Suppose that $1 = e_1 + \cdots + e_n$ where e_i is in A and $e_i e_j = \delta_{ij}$ for all i and j . (δ_{ij} equals 1 or 0 depending upon whether $i = j$ or not.) Let $A_i = Ae_i = \{\text{all } ae_i \text{ where } a \text{ is in } A\}$. Prove:

- (a) A_i is a left ideal of A for each i .
- (b) If a is any member of A then a is uniquely expressible in the form $a = \sum a_i$ where $a_i \in A_i$.

2. Let $f(x) = x^4 + x + 1$ be a polynomial over $\mathbb{F} = GF(2)$, the field with two members.

- (a) Show that $f(x)$ is irreducible in $\mathbb{F}[x]$.
- (b) Let K be the splitting field of $f(x)$ over \mathbb{F} . How many members does K have?
- (c) Describe an automorphism of K over \mathbb{F} having the maximum possible order in the Galois group of K over \mathbb{F} .
- (d) Find a subfield of K distinct from \mathbb{F} and K . List its elements as polynomials in α over \mathbb{F} where α is a root of $f(x)$ in K .

3. Let G be a group of order $7 \cdot 13 = 91$ and let H be a group of order $5 \cdot 7 \cdot 13 = 455$.

- (a) Prove that G is abelian. [Hint: Use the Sylow theorems.]
- (b) Prove that the Sylow 7- and Sylow 13-subgroups of H are both normal in H .
- (c) Is H abelian? If "yes," prove it. If "no," give an example of a nonabelian group of order 455.

PLEASE TURN OVER

PART B

1. Let V be the set of all rational numbers expressible in the form a/b where a and b are integers and b is odd. Show:

- (a) V is a subring of the rational numbers.
- (b) The field of quotients of V is the field of rational numbers.
- (c) Exhibit all the units of V .
- (d) Exhibit all the ideals of V and determine which are prime ideals and which are maximal ideals.
- (e) Prove V/M , where M is a maximal ideal of V , is isomorphic to $\mathbb{Z}_n (= \mathbb{Z}/n\mathbb{Z})$ for some n . Which n ?

2. Let \mathbb{Q} be the field of rational numbers. An absolute value on \mathbb{Q} is a real-valued function $|a|$ having the following properties:

- (1) $|a| \geq 0$ and $|a| = 0$ if and only if $a = 0$.
- (2) $|ab| = |a||b|$.
- (3) $|a + b| \leq |a| + |b|$.

Suppose that $|n| \leq 1$ for all natural numbers n . Show:

- (a) $|a + b| \leq \max\{|a|, |b|\}$ for all a and b .
- (b) Either $|a| = 1$ for all nonzero a or there is a prime number p such that, if $a = p^r m/n$, with m and n relatively prime to p and to each other while r is an integer, then $|a| = |p|^r$.

3. Recall that an ordered field is a field K together with a distinguished subset P (the “positive” elements) with the properties:

- (1) For all a in K exactly one of the following holds: a is in P , $-a$ is in P , or $a = 0$.
- (2) If a and b are in P , then so are $a + b$ and ab .

Show:

- (a) Any ordered field has characteristic zero.
- (b) The rational numbers can be ordered in exactly one way.
- (c) Any subfield of an ordered field can be ordered by an order induced by the larger field.

4. Describe, up to isomorphism, all groups of order 27. Describe the two nonabelian groups in terms of generators and defining relations.

1. Prove that every group of order $1645 = 5 \cdot 7 \cdot 47$ is abelian and cyclic.

2. Let $\mathcal{B} = \{v_1, \dots, v_m\}$ be a basis over \mathbb{Q} for the m -dimensional vector space V . Using \mathcal{B} , we identify the vectors in V with $m \times 1$ column vectors over \mathbb{Q} :

$$v = \alpha_1 v_1 + \dots + \alpha_m v_m \quad \longleftrightarrow \quad v_{\mathcal{B}} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}.$$

Let A be a symmetric $m \times m$ rational matrix. Then with respect to the basis \mathcal{B} , A defines a “symmetric bilinear form” $\langle \cdot, \cdot \rangle$ from $V \times V$ to \mathbb{Q} by

$$\langle u, v \rangle = {}^t u_{\mathcal{B}} A v_{\mathcal{B}} \quad \text{for all } u, v \in V.$$

(Here ${}^t u_{\mathcal{B}}$ denotes the transpose of the matrix $u_{\mathcal{B}}$). Note that $\langle u, v \rangle = \langle v, u \rangle$. For a subspace W of V , let W^{\perp} denote the subspace of V given by

$$W^{\perp} = \{v \in V : \langle v, w \rangle = 0 \text{ for all } w \in W\}.$$

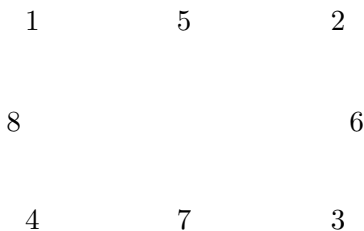
- Show that $V = V^{\perp} \oplus W$ for some subspace W which satisfies $W^{\perp} \cap W = \{0\}$.
- Suppose W is a subspace of V such that $W^{\perp} \cap W = \{0\}$. Show that there is some $x \in W$ such that $\langle x, x \rangle \neq 0$. [Hint: Argue that for $w \in W$, we can find some $w' \in W$ such that $\langle w, w' \rangle \neq 0$; now expand $\langle w + w', w + w' \rangle$.]
- Suppose still that W is a subspace of V such that $W^{\perp} \cap W = \{0\}$. Let $x \in W$ satisfy $\langle x, x \rangle \neq 0$. Show that $W = \mathbb{Q}x \oplus W'$ where $\langle x, w' \rangle = 0$ for all $w' \in W'$.
- FACT: Induction on $r = \dim W$ and (c) may be used to show that $V = V^{\perp} \oplus \mathbb{Q}x_1 \oplus \dots \oplus \mathbb{Q}x_r$, where $\langle x_i, x_i \rangle \neq 0$ and $\langle x_i, x_j \rangle = 0$ whenever $i \neq j$. Use this fact to show that for some nonsingular matrix S , ${}^t S A S = D$ where D is a diagonal matrix of rank $r = \dim W$.

3. Let G be a finite group of permutations of order N acting on s symbols. Let G_P denote the subgroup of G consisting of all elements fixing a given letter P .

- Let m be the number of elements in the transitivity class (orbit) containing P . Show that $|G_P| m = N$ where $|G_P|$ denotes the order of the subgroup G_P .
- Suppose that P and Q are in the same transitivity class. Show that G_P and G_Q are isomorphic groups.
- Let $\sigma(g)$ stand for the number of symbols left fixed by an element g in the group and let t be the number of transitivity classes under G . Show that

$$\sum_{g \in G} \sigma(g) = tN.$$

- Let G be the symmetry group of the rectangle shown below whose vertices are labelled 1, 2, 3, 4 and the midpoints of whose sides are labelled 5, 6, 7, 8. G is a Klein 4-group. Use its realization as a permutation group on the 8 points $\{1, 2, \dots, 8\}$ to illustrate the theorem in part (c).



4. Consider the ring $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$. In answering the following questions, you may want to use the “norm”: $N(a + b\sqrt{-3}) = a^2 + 3b^2$.

- What are the units in $\mathbb{Z}[\sqrt{-3}]$?
- Find all factorizations into irreducible elements of the number 4 in this ring, showing that $\mathbb{Z}[\sqrt{-3}]$ is not a Unique Factorization Domain. Is it a Euclidean domain? Explain.
- Test 5 and 7 to see if they are irreducible in $\mathbb{Z}[\sqrt{-3}]$.
- Give an example of an element of $\mathbb{Z}[\sqrt{-3}]$ which is irreducible but not prime.

5. Let $g(x) = x^7 - 1 \in \mathbb{Q}[x]$, and let K be a splitting field for $g(x)$ over \mathbb{Q} .

- Show that $g(x) = (x - 1)h(x)$ where $h(x)$ is irreducible in $\mathbb{Q}[x]$. [Hint: Study $h(x + 1)$ by first writing $h(x) = g(x)/(x - 1)$. Use Eisenstein’s criterion to show $h(x + 1)$ is irreducible.]
- Show that $G = \text{Gal}(K/\mathbb{Q})$ is cyclic of order 6, and has as generator the map that takes $r \rightarrow r^3$ for any root r of $g(x)$.
- Let ω be a complex 7th root of 1. Let

$$x_1 = \omega + \omega^2 + \omega^4, \quad x_2 = \omega + \omega^6.$$

Find subgroups H_1, H_2 of G such that $\mathbb{Q}(x_1)$ is the fixed field of H_1 and $\mathbb{Q}(x_2)$ is the fixed field of H_2 . Find $[\mathbb{Q}(x_1) : \mathbb{Q}]$ and $[\mathbb{Q}(x_2) : \mathbb{Q}]$.

- Show that, besides $\mathbb{Q}, \mathbb{Q}(\omega), \mathbb{Q}(x_1)$ and $\mathbb{Q}(x_2)$, there are no fields M with $\mathbb{Q} \subset M \subset \mathbb{Q}(\omega)$. (Here \subset denotes proper containment.)

6. Let $h(x) = x^4 + 1 \in \mathbb{Q}[x]$, and let L be a splitting field for $h(x)$ over \mathbb{Q} .

- Show that the four complex numbers $\pm \frac{\sqrt{2}}{2}(1 \pm i)$ are the four roots of $h(x)$ in \mathbb{C} .
- Find an $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$.
- Describe all elements of $G = \text{Gal}(L/\mathbb{Q})$ as permutations of the roots of $h(x)$.
- Find all intermediate fields M between L and \mathbb{Q} ; for each such field M find a subgroup H of G such that M is the fixed field of H and $H = \text{Gal}(L/M)$. Which of the extensions M are normal over \mathbb{Q} ?

1. Recall that a finite group G is called *solvable* if there is a sequence of groups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$$

such that for $i = 1, \dots, n$, G_i is normal in G_{i-1} and G_{i-1}/G_i is abelian.

- (a) Let p be a prime number, and a a positive integer. Show that any group of order p^a is solvable.
- (b) Let p and q be 2 distinct prime numbers, and a and b be any 2 positive integers. Show that any group of order $p^a q^b$ is solvable.

2. Let \mathbb{R}^3 denote the 3-fold Cartesian product of the real numbers with itself. We will consider all its elements as column vectors.

- (a) Recall that the standard inner product of 2 vectors v and w in \mathbb{R}^3 is given by $v \cdot w = {}^t v w$, where t denotes the transpose. Prove that if w_1 and w_2 are vectors in \mathbb{R}^3 , and for all v in \mathbb{R}^3 , $v \cdot w_1 = v \cdot w_2$, then $w_1 = w_2$.
- (b) Let E denote the symmetric matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

and define $\phi(\cdot, \cdot)$ to be the symmetric bilinear form on \mathbb{R}^3 given by

$$\phi(v, w) = v \cdot Ew = w \cdot Ev$$

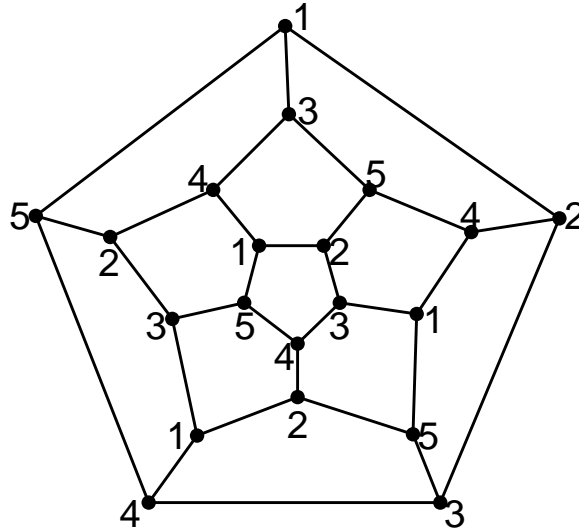
(where the second equality follows from the symmetry of E).

Prove that for an arbitrary 3×3 matrix A , the following conditions are equivalent:

- (i) $\phi(Av, Aw) = \phi(v, w)$ for all $v, w \in \mathbb{R}^3$.
 - (ii) $\det A = \pm 1$, and A satisfies: If $\phi(v, v) = 0$, then $\phi(Av, Av) = 0$.
 - (iii) The columns c_i of A satisfy: $\phi(c_1, c_1) = \phi(c_2, c_2) = -\phi(c_3, c_3) = 1$ and $\phi(c_i, c_j) = 0$ for $i \neq j$.
 - (iv) ${}^t AEA = E$.
- (c) Let us call a matrix A *hyperbolic* if it satisfies any (hence all) of the conditions in part (b). Prove that the hyperbolic 3×3 real matrices form a group.

3. Recall that a *regular dodecahedron* is a convex polygon whose faces comprise twelve regular pentagons, symmetrically arranged. In this problem, we will let G stand for the group of orientation-preserving rigid motions of the regular dodecahedron. In a coordinate system centered at the center of the dodecahedron, each element of G is a rotation centered at the origin. In particular, elementary geometric considerations show that G consists of elements of 4 types: (i) The identity; (ii) A two-fold rotation that fixes the midpoints of 2 antipodal edges; (iii) A three-fold rotation about each of its twenty vertices; and (iv) Five-fold rotations that cyclically permute each of its twelve pentagons.

To make this clearer, below is the *Schlegel diagram* of the dodecahedron (a combinatorially correct, but metrically inaccurate, representation).



Note that the vertices of the Schlegel diagram have been numbered from 1 to 5. You may assume the slightly-painful-to-verify fact that every element of G permutes the labels in the Schlegel diagram above in a consistent manner. That is to say, if vertices A and B have the same label, and if $g \in G$, then $g(A)$ and $g(B)$ also have the same labels. In other words, G acts on the set of labels. The purpose of this exercise is to show that G is isomorphic to the alternating group A_5 on five letters.

- (a) Make a table showing the number of elements in G of order 1, of order 2, of order 3, and 5.
- (b) Do the same thing for A_5 .
- (c) Prove that G is isomorphic to A_5 .

4. Let A be a commutative ring. An element $a \in A$ is called *nilpotent* if $a^n = 0$ for some positive integer n . Let

$$N = \{a \in A : a \text{ is nilpotent}\}.$$

- (a) Show that N is an ideal.
- (b) Let \mathfrak{p} be a prime ideal in A . Show that $N \subseteq \mathfrak{p}$.
- (c) Show that A/N contains no nonzero nilpotent elements.

PLEASE TURN OVER

5. Let R be a ring. Recall that a sequence of R -modules A , B , and C with R -module homomorphisms f and g

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is called *exact* if the image of f is equal to the kernel of g . Also recall that a diagram of R -modules A , B , C , and D , with R -module homomorphisms f, g, h , and i

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow h & & \downarrow g \\ C & \xrightarrow{i} & D \end{array}$$

is called *commutative* if $g \circ f = i \circ h$.

Consider the following diagram of modules and homomorphisms, where each square is commutative, and each sequence in the top and bottom rows is exact:

$$\begin{array}{ccccccc} A_1 & \xrightarrow{g_1} & A_2 & \xrightarrow{g_2} & A_3 & \xrightarrow{g_3} & A_4 \\ \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \downarrow f_4 \\ B_1 & \xrightarrow{h_1} & B_2 & \xrightarrow{h_2} & B_3 & \xrightarrow{h_3} & B_4 \end{array}$$

Prove that if f_1 is surjective, and f_2 and f_4 are injective, then f_3 is injective.

6. Let $K = \mathbb{F}_q$ be the finite field with q elements, and let $K(x)$ denote the field of rational functions over K in the variable x . Let $G = GL_2(K)$ denote the group of 2×2 invertible matrices with entries in K . If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in G , then we associate to g an automorphism $\phi(g)$ of $K(x)$ which leaves K pointwise fixed, and

$$\phi(g)(x) = \frac{ax + b}{cx + d}.$$

You may assume the well-known fact that the map ϕ from G into the group of automorphisms of $K(x)$ is a homomorphism.

- Show that the order of G is $q^4 - q^3 - q^2 + q$.
- Let $H = \phi(G)$. Show that the order of H is $q^3 - q$.
- Use field theory to show that $f = \frac{(x^{q^2} - x)}{(x^q - x)}$ is relatively prime to $x^q - x$.
- Prove that the fixed field of H is the field $K(y)$, where

$$y = \frac{(x^{q^2} - x)^{q+1}}{(x^q - x)^{q^2+1}} = \frac{f^{q+1}}{(x^q - x)^{q^2-q}}.$$

[Hint: Use the fact that G is generated by the set of matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

as a varies over all nonzero elements of K .]

DO ANY 5 OF THE FOLLOWING 7 PROBLEMS

1. Let C denote the unit circle, $x^2 + y^2 = 1$, in the real plane. Let E be the point $(1, 0) = (\cos(0), \sin(0))$ on C and let $A = (\cos(\alpha), \sin(\alpha))$ and $B = (\cos(\beta), \sin(\beta))$ be an arbitrary pair of points on C . Define a binary operation on C as follows: $A * B = U$ is the second point of intersection on C and the straight line through E parallel to the straight line through A and B . (When $A = B$, the line through A and B is the line tangent to C at A .)

Prove: This operation induces the structure of an abelian group on C with E as the identity element.

[Hint: All of the group laws except for associativity are easy to verify. In order to show associativity you must show that C is isomorphic to the circle group $\mathbb{R}/2\pi\mathbb{Z}$ and, thus, note that associativity of the binary operation is inherited]

2. Using the result of Problem 1, show that if C is the ellipse $3x^2 + 5y^2 = 1$ in the real plane then the geometric operation described above makes C into an abelian group. Specifically, let O be an arbitrary point on C - this will be the identity element of the group. If A and B are two points on C , then $A + B$ is the second point of intersection of the line through O that is parallel to the line through A and B .

3. Let R be an associative ring with identity element such that $a^2 = a$ for all a in R . Show that R is necessarily commutative and that $a = -a$ for all a .

4. (a) Give an example of a homomorphism of rings $f : R \rightarrow S$ with multiplicative identities 1_R and 1_S such that $f(1_R)$ does not equal 1_S .
(b) If $f : R \rightarrow S$ is an epimorphism of rings with identity, show that $f(1_R) = 1_S$.
(c) Now assume only that $f : R \rightarrow S$ is a homomorphism of rings both of which have multiplicative identities and that there is a unit u of R such that $f(u)$ is a unit in S . Prove that $f(1_R) = 1_S$ and that $f(u^{-1}) = f(u)^{-1}$.

5. Let G be a group of order 10,000 having a normal subgroup K of order 100. Show that G has a normal subgroup of order 2500.

6. Let $p(x) = x^n - 1$ and suppose that $p(x)$ splits in the field K . Let G be the set of all roots of $p(x)$ in K .

- (a) Show that any finite subgroup of K^* (the multiplicative group of K) is cyclic.
(b) Show that G is a cyclic group under multiplication.
(c) What is the order of G ?

Note: Characteristic 0 and p must be handled separately.

7. Using the fact (obtained in Problem 6) that G is cyclic:

- (a) Show that the field $\mathbb{Q}(G)$ is an abelian extension of the field \mathbb{Q} of rational numbers.
(b) Show that the Galois group of $\mathbb{Q}(G)$ over \mathbb{Q} in the case of $p(x) = x^8 - 1$ is the Klein 4-group.

Note: $\mathbb{Q}(G)$ is the field extension of \mathbb{Q} obtained by adjoining the elements of G .

DO 6 OF THE FOLLOWING 7 PROBLEMS

1. Let G be a group and $\text{Aut}(G)$ the group of automorphisms of G . Let C be a characteristic subgroup of G , i.e., C is a subgroup of G such that $\alpha(C) = C$ for all $\alpha \in \text{Aut}(G)$. Now let

$$B = \{\beta \in \text{Aut}(G) : \beta(c) = c \text{ for all } c \in C\}.$$

- (a) Show that B is a normal subgroup of $\text{Aut}(G)$.
 (b) Suppose that p is a prime integer and G is a group such that $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Show that

$$\text{Aut}(G) \simeq GL_2(\mathbb{Z}/p\mathbb{Z}) = \{\text{invertible } 2 \times 2 \text{ matrices with entries from } \mathbb{Z}/p\mathbb{Z}\}.$$

2. Prove that every group of order 45 is abelian.

3. Let $G = \{a_1, \dots, a_n\}$ be a finite abelian group of order n and with identity e .

- (a) Prove that $(\prod_{i=1}^n a_i)^2 = e$.
 (b) Prove that if G has no elements of order 2 or if G has more than one element of order 2 then

$$\prod_{i=1}^n a_i = e.$$

[Hint: Consider the subgroup $\{x \in G : x^2 = e\}$.]

- (c) Prove that if G has exactly one element x of order 2, then

$$\prod_{i=1}^n a_i = x.$$

- (d) Prove *Wilson's Theorem*, which states that if p is a prime integer then

$$(p-1)! \equiv -1 \pmod{p}.$$

4. (a) Let $\mathbb{Z}[x]$ be the ring of polynomials in the indeterminate x with integer coefficients. Find an ideal in $\mathbb{Z}[x]$ which is not principal. Justify your result.
 (b) Find a nonzero prime ideal in $\mathbb{Z}[x]$ which is not maximal. Justify your result.
 (c) Let R be a principal ideal domain. Prove that a proper nonzero ideal in R is a maximal ideal if and only if it is prime.

5. Let $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ where p is a prime; take $a \in \mathbb{F}$, $a \neq 0$, and let x be an indeterminate.

- (a) Show that if α is a root of $x^p - x - a$ then so is $\alpha + 1$.
 (b) Show that $x^p - x - a$ is irreducible in $\mathbb{F}[x]$.
 (c) Let K be a splitting field over \mathbb{F} for $x^p - x - a$. Compute the Galois group of K over \mathbb{F} .

6. Let \mathbb{F} be a finite field with q elements and characteristic $p > 2$.

- (a) Show that exactly half the nonzero elements of \mathbb{F} are squares in \mathbb{F} . [Hint: Consider the mapping $a \mapsto a^2$.]
- (b) Show that for $a \in \mathbb{F}^\times = \{x \in \mathbb{F} : x \neq 0\}$, we have $a = b^2$ for some $b \in \mathbb{F}$ if and only if a is the root of the polynomial $X^{\frac{q-1}{2}} - 1$.
- (c) Show that -1 is a square in the field $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod{4}$. (Recall that $p \in \mathbb{Z}_+$ is an odd prime.)

7. Assumptions: Let V be a vector space over a field F and W a subspace of V ; suppose that $\dim_F V = n < \infty$ and $\dim_F W = m < n$ (where $\dim_F V$ denotes the dimension of V as a vector space over F). Thus each element $\alpha \in F$ acts on V ; notice that this action is a linear transformation on V . Let \mathcal{R} be a commutative ring of linear transformations on V such that (i) $F \subseteq \mathcal{R}$, and (ii) for $T \in \mathcal{R}$ we have $T(W) \subseteq W$. Let $\mathcal{S} = \{T \in \mathcal{R} : T(V) \subseteq W\}$. Note that \mathcal{S} is an ideal of \mathcal{R} .

Prove:

- (a) Show that $\alpha \mapsto \alpha + \mathcal{S}$ gives an embedding of the field F into the ring \mathcal{R}/\mathcal{S} ; using the fact that a ring containing a field is a vector space over that field, show that \mathcal{R}/\mathcal{S} is a vector space over F .
- (b) Show that V/W is a module over \mathcal{R}/\mathcal{S} .
- (c) Suppose \mathcal{S} is a maximal ideal of \mathcal{R} . Show that

$$\dim_F \mathcal{R}/\mathcal{S} \cdot \dim_{\mathcal{R}/\mathcal{S}} V/W = \dim_F V/W.$$

ALGEBRA PRELIM

AUGUST 1990

ANSWER 2 OF THE QUESTIONS OF PART I AND 4 OF THE QUESTIONS OF PART II

PART I

1. Show that the center of a nonabelian group of order p^3 has order p .

2. Let G be the infinite dihedral group $= \langle v, t \rangle$ with generators v and t where t has infinite order, v is of order two, and $vt = t^{-1}v$. Let H be a subgroup of index 2 in G and let $T = \langle t^2 \rangle$, a normal subgroup.
 - (a) Show that $T \subseteq H$. (You may use the fact that H must be normal because it has index 2.)
 - (b) Describe the quotient group G/T .
 - (c) List the subgroups of index 2 in G/T .
 - (d) Use an appropriate correspondence theorem to find all subgroups of index 2 in G (note any subgroup may be described by listing its generators).

3. Inside the symmetric group S_4 , let

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

where e is the identity.

- (a) Show that H is a normal subgroup of S_4 , and that A_4/H is cyclic.
- (b) Show that H is its own centralizer in S_4 .
- (c) By considering the homomorphism

$$\varphi : S_4 \rightarrow \text{Aut}(H) \quad \text{defined by} \quad \varphi(s) = \{h \rightarrow shs^{-1}\},$$

show that

$$\frac{S_4}{H} \simeq \text{Aut}(H) \simeq S_3.$$

PLEASE TURN OVER

PART II

4. Let \mathbb{Z}_2 denote the field with two elements.
- If f is an irreducible polynomial of degree 17 over \mathbb{Z}_2 , how many elements are there in the splitting field of f ?
 - How many irreducible polynomials of degree 17 are there over \mathbb{Z}_2 ?
5. Let $R = \mathbb{Z}[x, y]$.
- Prove or disprove: The ideal $I = (x, y)$ is a prime ideal in R .
 - Find all maximal ideals in R which contain I .
 - Prove or disprove: The ideal $J = (y^2 - x^3)$ is a prime ideal in R .
6. (a) Let $\phi : V \rightarrow V$ be a linear transformation of a vector space V over a field K . Let E be a collection of eigenvectors of ϕ whose eigenvalues are distinct. Prove that E is a linearly independent set.
- (b) Suppose that $\phi : V \rightarrow V$ is a linear transformation of a vector space V where $\dim V = n$. Suppose that ϕ has n distinct eigenvalues. Prove that there is a basis B of V such that the matrix representation of ϕ with respect to B is a diagonal matrix.
7. Let $f(x) = x^5 - 5$ be a polynomial defined over the rational field \mathbb{Q} . Let E be the splitting field of f .
- Find the degree of E over \mathbb{Q} .
 - Give the structure of the Galois group of E over \mathbb{Q} presenting generators and relations.
8. Let F be a field. Let V be the subgroup of the multiplicative group of the reals given by
- $$V = \{2^n : n \in \mathbb{Z}\}.$$
- F is called *isosceles* if there exists a surjective map $f : F \rightarrow V \cup \{0\}$ with the following properties:
- $f(0) = 0$ and $f(\alpha) > 0$ if $\alpha \neq 0$.
 - $f(\alpha\beta) = f(\alpha)f(\beta)$ for all $\alpha, \beta \in F$.
 - $f(\alpha + \beta) \leq \max\{f(\alpha), f(\beta)\}$.
- Suppose F is an isosceles field. Let $R = \{\alpha \in F : f(\alpha) \leq 1\}$. Show that R is a ring with identity.
 - Let $P = \{\alpha \in F : f(\alpha) < 1\}$. Prove that P is a prime ideal of R .
 - Show that P is a principal ideal.

ALGEBRA PRELIM

JANUARY 1990

DO TWO OF THE FIRST THREE PROBLEMS AND FOUR OF THE LAST FIVE

1. Let H be a proper subgroup of a finite group G . Show that G is not the union of all the conjugates of H . [Hint: How many conjugates does H have?]

2. Classify (up to isomorphism) all groups of order $286 = 2 \times 11 \times 13$.

3. If G is a group, and $x \in G$, then the *inner automorphism* of G determined by x is the automorphism $\alpha_x : G \rightarrow G$, $\alpha_x(g) = x^{-1}gx$ for $g \in G$. If an automorphism is not an inner automorphism, then it is called an *outer automorphism*.
 - (a) Does the set of all inner automorphisms of G form a group? Justify your answer, i.e., either prove the set is a group, or give a counterexample.
 - (b) Does the set of all outer automorphisms along with the identity automorphism form a group? Justify your answer.
 - (c) Show that every finite abelian group, with the exception of one abelian group, has an outer automorphism. What is the exceptional abelian group?

4. Let R be a commutative ring with unity. We call an element $e \in R$ an *idempotent* if $e^2 = e$. Suppose M is an R -module, and e is an idempotent of R . Set

$$M_1 = \{em : m \in M\}, \quad M_2 = \{(1 - e)m : m \in M\}.$$
 - (a) Show that M_1 and M_2 are submodules of M .
 - (b) Show that $M = M_1 \oplus M_2$.

5.
 - (a) Give an example of a non-principal ideal I in a Noetherian integral domain A .
 - (b) Give an example of a not finitely generated ideal I in an integral domain A .
 - (c) Give an example of a Unique Factorization Domain which is not a Principal Ideal Domain.

PLEASE TURN OVER

6. Let $f(x) = x^4 + ax^2 + b$ be an irreducible polynomial over \mathbb{Q} , with roots $\pm\alpha, \pm\beta$ and splitting field K . Show that $\text{Gal}(K/\mathbb{Q})$ is isomorphic to a subgroup of the dihedral group D_4 (this is the noncommutative group of order 8 which is not isomorphic to the quaternion group) and therefore is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or D_4 .

7. Let p be an odd prime, and let $\zeta = e^{2\pi i/p}$. Recall that the map

$$a \mapsto (\sigma_a : \zeta \rightarrow \zeta^a)$$

gives an isomorphism between $(\mathbb{Z}/p\mathbb{Z})^\times$ and the Galois group of $\mathbb{Q}(\zeta)$ over \mathbb{Q} .

Recall also that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group, so has a unique subgroup S of index 2 consisting of the elements which are squares. Let χ be the composite homomorphism

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times / S \simeq \{\pm 1\} \\ & \searrow \chi & \nearrow \\ & & \end{array}$$

In other words,

$$\chi(t) = \begin{cases} 1 & \text{if } t \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^\times \\ -1 & \text{if } t \text{ is not a square in } (\mathbb{Z}/p\mathbb{Z})^\times. \end{cases}$$

Let $g = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(t)\zeta^t$.

- Show that $\sigma_a(g) = \chi(a)^{-1}g = \chi(a)g$, for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.
- Show that $g^2 \in \mathbb{Q}$, but $g \notin \mathbb{Q}$.
- Show that $\mathbb{Q}(g)$ is the unique degree 2 extension of \mathbb{Q} contained in $\mathbb{Q}(\zeta)$.

8. Let p_1, p_2, \dots, p_n be distinct primes. Show that $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$ is of degree 2^n .

1. Let k be an arbitrary field and let $k(z)$ be the field of rational functions in one variable over k . Let a_1, \dots, a_n be distinct elements of k . Let e_1, \dots, e_n be natural numbers (i.e., $e_j > 0$). Let L be the set of all elements $R(z) = f(z)/g(z)$ of $k(z)$ satisfying (i) $\gcd(f, g) = 1$, (ii) the roots of $g(z)$ in the algebraic closure of k are among the points a_1, \dots, a_n and have multiplicities at most e_1, \dots, e_n , respectively, and (iii) $\deg f(z) \leq \deg g(z)$.

- (a) Show L is a vector space over k .
- (b) Find an explicit basis for L over k .
- (c) Prove $\dim_k L = e_1 + \dots + e_n + 1$.
- (d) What can be said if $\deg f(z) \geq \deg g(z)$?

2. Let C be the hyperbola $xy = 1$ in the real plane. Let (a, b) and (c, d) be points on C (i.e., $ab = cd = 1$). Let L be the line through (a, b) and (c, d) . When $(a, b) = (c, d)$ then L is assumed to be the line tangent to C at that point. Next let M be the line through $(1, 1)$ parallel to L . Let (x, y) be the other point on C where M intersects C . When M is tangent to C then (x, y) is set equal to $(1, 1)$. Define a binary operation on C by setting $(a, b) \cdot (c, d) = (x, y)$. Show:

- (a) C is an abelian group under this binary operation with $(1, 1)$ as identity element.
- (b) C is isomorphic to \mathbb{R}^\times (the multiplicative group of nonzero real numbers).

[Hint: Set up the isomorphism first and use it to show that all of the group properties on C are inherited from \mathbb{R}^\times .]

3. (a) Let G be a group and let H be a normal subgroup. Suppose that every element of G/H has finite order and every element of H also has finite order. Show that every element of G has finite order.
- (b) Show that no group of order 56 is simple.

4. Let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n . Let $G = \mathbb{Z}_{45} \oplus \mathbb{Z}_{54} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{10}$.

- (a) What is the order of the largest cyclic subgroup of G ?
- (b) How many elements of order 3 are there in G ?

5. Let $f(x) = (x^2 - 3)(x^3 - 5)$ and $g(x) = (x^2 + 3)(x^3 - 5)$. Let K and L be the splitting fields, respectively, of $f(x)$ and $g(x)$ over the rational numbers, \mathbb{Q} .

- (a) Find generators for K and L over \mathbb{Q} .
- (b) Find the degrees $[K : \mathbb{Q}]$ and $[L : \mathbb{Q}]$.

1. Let G be a finite group and let H be a subgroup of G of index n . Show: there exists a normal subgroup H^* of G with the properties that $H^* \leq H$ and $[G : H^*] \leq n!$. [Hint: Construct a homomorphism of G into the symmetric group S_n whose kernel is contained in H .]

2. Let p be a rational prime and let $q = p^t$. Let $GF(p)$ and $GF(q)$ be the fields with p and q elements, respectively. Let $T : GF(q) \rightarrow GF(p)$ be the trace map (i.e., $T(x)$ equals the sum of the conjugates of x). Let $\Phi : GF(q) \rightarrow GF(q)$ be defined by $\Phi(x) = x^p - x$. Show:

- (a) Φ is a homomorphism of the additive group $GF(q)$.
- (b) The kernel of Φ is $GF(p)$.
- (c) The image of Φ equals the kernel of T .
- (d) T maps $GF(q)$ onto $GF(p)$.

3. Let $f_m(x) = (x - \mu_1) \cdots (x - \mu_r)$ where the roots range over the (complex) primitive m^{th} roots of unity. Show:

- (a) The coefficients of f_m are rational integers.
- (b) If p is a rational prime not dividing m then $f_m(x^p) = f_m(x)f_{pm}(x)$.
- (c) f_m is irreducible over \mathbb{Q} (the rational numbers).

4. A field is said to be *formally real* if the equation $x_1^2 + \cdots + x_n^2 = -1$ is not solvable in the field. A field is said to be *real closed* if it is formally real and does not possess a proper, algebraic, formally real extension. Show:

- (a) A formally real field has characteristic zero.
- (b) If K is formally real, with algebraic closure M then there exists a real closed field L such that $K \leq L \leq M$.
- (c) A real closed field K is ordered in exactly one way (i.e., there is a subset P of K such that (i) for all a in K exactly one of the following holds: $a = 0$, a is in P , $-a$ is in P and (ii) if x and y are in P then so are $x + y$ and xy). Moreover, the set of positive elements of K is precisely the set of nonzero squares. [Hint: Show that if a nonzero element a of the field is not a square then $-a$ is a square.]
- (d) An example of a formally real subfield K of \mathbb{C} (the complex numbers) which is algebraic over \mathbb{Q} (the rational numbers) but which is not itself a subfield of \mathbb{R} (the real numbers).

1. Determine the number of (isomorphism classes of) groups of order 21. (Justify your answer.)

2. Let R be an associative ring with multiplicative identity 1.
 - (a) Let $x \in R$ be arbitrary. Show that $\ell(x) = \{z \in R : zx = 0\}$ is a left ideal in R .
 - (b) Let x be any element of R that has a multiplicative left inverse y in R .
 - (i) Prove that y is unique iff $\ell(x) = 0$.
 - (ii) Prove that y is unique iff x is a unit in R .

3. Let L be a free \mathbb{Z} -module of rank 2 contained in \mathbb{C} . Let $\{w_1, w_2\}$ be a \mathbb{Z} -basis for L and assume that $u = w_1/w_2$ is not real. Assume also that there exists a complex number z , not in \mathbb{Z} , such that $zL \subseteq L$. Show the following facts:
 - (a) The minimal polynomial for u over \mathbb{Q} is quadratic (hence u is algebraic).
 - (b) If w is any complex number for which $wL \subseteq L$, then $w \in \mathbb{Q}(u)$ and satisfies a quadratic equation of the form $w^2 + rw + s = 0$ where r and s are in \mathbb{Z} .
 - (c) If R denotes the set of all complex numbers w for which $wL \subseteq L$, then R is a subring of $\mathbb{Q}(u)$ and L is isomorphic to an ideal of R .

4. Let F be a field and let $R = F[[x]]$ be the ring of formal power series in one variable with coefficients in F .
 - (a) Describe the units in R . (Justify your answer.)
 - (b) Show that every nonzero ideal in R is of the form $x^k R$, $k \in \mathbb{Z}$, $k \geq 0$.
 - (c) Show that x is the unique prime element in R , up to associates.

1. Determine up to isomorphism all groups of order 8.
2. Let G be a finite group and $f : G \rightarrow G$ be an automorphism of G . If $f(x) = x$ implies $x = e$, and $f^2 = f \circ f$ equals the identity map, show that G is abelian. [Hints: Prove that every element in G has the form $x^{-1}f(x)$ and that if $\phi(x) = x^{-1}$ for all $x \in G$ is an isomorphism, then G is abelian.]
3. (a) Let R be a ring with 1. State the axioms for a unitary left R -module M .
(b) Let M be a cyclic unitary left R -module with generator m , i.e., $M = R\langle m \rangle$. Let $J = \{r \in R : rm = 0\}$. Show that J is a left ideal of R .
(c) Regarding both R and J as left R -modules, show that $R/J \cong M$, i.e., R/J and M are isomorphic as left R -modules.
4. Find the Galois group of $x^5 - 3$ over \mathbb{Q} . Give the order of the group, find the splitting field and give a set of generators for the Galois group by describing their effect on the roots of the polynomial.
5. (a) Let x be an indeterminate (transcendental) over the complex numbers \mathbb{C} and suppose that $r(x) = \frac{p(x)}{q(x)}$ where $p(x)$ and $q(x)$ are elements of $\mathbb{C}[x]$ and are relatively prime. Define $\deg r(x) = \max\{\deg p(x), \deg q(x)\}$. Show that if $\deg r(x) \geq 1$, then $r(x)$ is transcendental over \mathbb{C} and that $\mathbb{C}(x)$ is an algebraic extension of $\mathbb{C}(r(x))$ of degree equal to $\deg r(x)$.
(b) Show that there is an automorphism ϕ of $\mathbb{C}(x)$ fixing \mathbb{C} defined by $\phi(x) = r(x)$ precisely if $r(x) = \frac{ax+b}{cx+d}$ where $ad - bc \neq 0$ (i.e., the automorphisms of $\mathbb{C}(x)$ fixing \mathbb{C} correspond to the set of linear fractional transformations).
6. Prove that the integral domain Γ of Gaussian integers (i.e., complex numbers of the form $a + bi$, with a and b integers) is a unique factorization domain.

1. Show that every group of order 77 is cyclic.

2. Let G be the direct sum of cyclic groups of order m and n where $m \mid n$. Let G be written additively.
 - (a) Determine the order of the subgroup $G(m)$ consisting of elements x with $mx = 0$.
 - (b) Determine the order of the group of endomorphisms of G , i.e., the homomorphisms of G into itself.

3. Let R be a ring with identity and M a unitary R -module.
 - (a) If $m \in M$, show that $\{x \in R : xm = 0\}$ is a left ideal of R .
 - (b) Let A be a left ideal of R and $m \in M$. Show that $\{xm : x \in A\}$ is a submodule of M .
 - (c) Suppose it is given that M has no submodules other than $\{0\}$ and M itself (i.e., M is *irreducible*). Let $m_0 \in M$, $m_0 \neq 0$. Show that $A = \{x : xm_0 = 0\}$ is a maximal left ideal of R (that is, if A is contained properly in a left ideal B , then $B = R$).

4. An ideal I in a commutative ring R with identity is *primary* if for any a, b in R with $a \cdot b \in I$, if $a \notin I$, then $b^n \in I$ for some $n \geq 1$.
 - (a) Show that I is primary iff every zero divisor in R/I is nilpotent.
 - (b) Let $\sqrt{I} = \{x \in R : x^n \in I \text{ for some } n\}$. Prove that if I is a primary ideal, then \sqrt{I} is a prime ideal.
 - (c) When R is a principal ideal ring, show that I is primary iff $I = P^e$ for some prime ideal P with $e \geq 0$.

5. Let ω be a primitive 10^{th} root of unity in \mathbb{C} .
 - (a) Find the Galois group of $\mathbb{Q}(\omega)$ over \mathbb{Q} (where \mathbb{Q} is the field of rational numbers).
 - (b) Let Φ_n denote the n^{th} cyclotomic polynomial over \mathbb{Q} . What is the degree of Φ_{20} over \mathbb{Q} ?
 - (c) Using the notation of parts (a) and (b), determine how many factors there are and what are their degrees when Φ_{20} is factored into irreducible factors over $\mathbb{Q}(\omega)$.

DO FIVE OF THE SIX PROBLEMS

1. Let α be an element of the alternating group A_n . Prove that the number of conjugates of α in A_n (i.e., under conjugacy by the elements of A_n) is either the same as or only half as large as the number of conjugates of α in the symmetric group S_n that contains A_n .
2. Let G be a group of order $780 = 2^2 \cdot 3 \cdot 5 \cdot 13$ which is *not* solvable. What are the orders of its composition factors? Explain your reasoning. (You may assume without proof that all groups of order less than 60 are solvable.)
3. (a) Prove that prime elements in an integral domain are irreducible.
(b) Let D be a principal ideal domain. Prove that if P is a nonzero prime ideal in D , then P is a maximal ideal.
(c) Let $R[x]$ be the ring of polynomials in one indeterminate over an integral domain R . Prove that if $R[x]$ is a principal ideal domain, then R is a field.
4. Let R be a commutative ring (not necessarily with multiplicative identity). Prove that if the only ideals in R are (0) and R , then either:
 - (a) R is the zero ring: $R = \{0\}$,
 - (b) R contains a prime number p of elements, and $a \cdot b = 0$ for all $a, b \in R$, or
 - (c) R is a field.
5. (a) Let \mathbb{F}_p denote a finite field with p elements, where p is an arbitrary prime, x be transcendental over \mathbb{F}_p , $K = \mathbb{F}_p(x)$, and $f(z) = z^p - x \in K[z]$, where $K[z]$ is the ring of polynomials in a transcendental element z over the field K . Prove:
 - (i) $f(z)$ is irreducible in $K[z]$.
 - (ii) If θ is a root of $f(z)$ in its splitting field over K , then $K(\theta)$ is an inseparable (algebraic) extension of K .
(b) Prove: If F is a subfield of a field E such that $[E : F] = n = (\text{degree of } E \text{ over } F) < \infty$, x is transcendental over F , $f(x) \in F[x]$ is irreducible of degree $d \geq 1$ in $F[x]$ and $(d, n) = 1$, then $f(x)$ is irreducible in $E[x]$.
6. (a) Let \mathbb{Q} denote the field of rational numbers. Determine the subfield K of the complex field \mathbb{C} that is the splitting field over \mathbb{Q} of the polynomial $f(x) = x^4 - x^2 - 6$.
(b) Determine the Galois group $\text{Gal}(K/\mathbb{Q}) = \text{Gal}(f/\mathbb{Q})$ and all of its subgroups.

1. G is a finite group of order $2p$, where p is a positive odd prime number. You are given that x, y are elements of G of order $2, p$, respectively.

- (a) Prove from first principles (i.e., using only the notion of a group) that $xyx^{-1} = y^m$ for some integer m .
- (b) Prove that one may take $m = 1$ or $p - 1$.

2. There exists a simple group G of order 168. Prove that G is isomorphic to a subgroup of S_8 , the symmetric group on eight letters. [Hint: Consider Sylow subgroups of G .]

3. Let $R = \mathbb{Z}[x, y]$, where \mathbb{Z} denotes the ring of rational integers and x, y are algebraically independent over \mathbb{Z} . For each of the ideals I in R as defined below:

- (i) Briefly describe the quotient ring R/I . (If you wish, you may describe an isomorphic image.)
- (ii) Determine whether or not I is prime. (Justify your answer.)
- (iii) Determine whether or not I is maximal. (Justify your answer.)

- (a) $I = (y)$, the principal ideal generated by y in R .
- (b) $I = (y, 5, x^2 + 1)$, the ideal generated by the three elements $y, 5, x^2 + 1$ in R .
- (c) $I = (y, 3, x^2 + 1)$, the ideal generated by the three elements $y, 3, x^2 + 1$ in R .

4. Let $M \neq \{0\}$ be an arbitrary left R -module of an arbitrary ring $R \neq \{0\}$. M is called a *simple* left R -module if and only if its only proper left R -submodule is $\{0\}$. Prove:

- (a) If M is simple, then either
 - (i) $RM = \{0\}$ and M is finite of prime order, or
 - (ii) $RM \neq \{0\}$ and M is a unitary cyclic left R -module generated by each of its nonzero elements.
- (b) If either (i) or (ii) above holds, then M is simple.

5. Let $\mathbb{F} = GF(2)$, the field with two elements. Let K be a splitting field for $f(x) = x^4 + x + 1$ over \mathbb{F} . Let α be an element of K such that $f(\alpha) = 0$. Find all elements $\beta \in K$ such that $K = \mathbb{F}(\beta)$. (Express each β as a polynomial in α over \mathbb{F} of least possible degree.) Prove that your list is complete.

6. Determine the Galois group G of $x^6 - 3$ over \mathbb{Q} (the rational number field).

4. Let $w(x, y) = x^{m_1}y^{n_1} \cdots x^{m_r}y^{n_r}$, m_i and n_j are any integers (of any sign), different from 0 and $r \geq 1$. Find two permutations p and q of a finite set such that

$$w(p, q) = p^{m_1}q^{n_1} \cdots p^{m_r}q^{n_r}$$

is a permutation different from the identity.

5. (a) Consider the matrix

$$A = \frac{1}{25} \begin{bmatrix} 15 & 12 & -16 \\ -20 & 9 & -12 \\ 0 & 20 & 15 \end{bmatrix}$$

as a linear mapping from \mathbb{R}^3 into itself. You may assume without proof that this mapping is a rotation around a certain axis through an angle θ . Find the axis and find θ .

(b) Find two different square roots of A , one a rotation and one not. For full credit, include a numerical solution; up to 6 out of 8 points will be awarded for a geometric description and a description of how one would proceed in calculating \sqrt{A} , in lieu of the calculation itself.

6. In the following problem, you may assume the following fact, which holds for cubic polynomials over any field:

$$\text{if } x^3 + px + q = (x - \alpha)(x - \beta)(x - \gamma), \text{ then } [(\gamma - \alpha)(\gamma - \beta)(\beta - \alpha)]^2 = -4p^3 - 27q^2.$$

You may assume the fundamental facts of Galois theory, but apart from these assumptions, please base your proofs on fundamentals of field theory.

- (a) Prove that $f(x) = x^3 - 3x + 1$ is irreducible over the field \mathbb{Q} of rational numbers.
- (b) Prove that $f(x)$ has three distinct real roots (alias “zeros”). Let us call them α, β, γ with $\alpha < \beta < \gamma$.

1. Let Z_n denote the (additive) cyclic group of order n . Let $G = Z_{15} \oplus Z_9 \oplus Z_{54} \oplus Z_{50} \oplus Z_6$.
 - (a) What is the order of the largest cyclic subgroup in G ?
 - (b) How many elements are there of order 5?
 - (c) How many elements are there of order 25?
 - (d) How many subgroups are there of order 25?

2. Let $K = GF(p^n)$ be a finite field of characteristic p which has degree n over its prime field $GF(p)$.
 - (a) Prove that K has p^n elements.
 - (b) Prove that K is a Galois extension of $GF(p)$ and describe its Galois group.
 - (c) Prove: $GF(p^m)$ is (isomorphic to) a subfield of $GF(p^n)$ if and only if m divides n . Show that in this case $GF(p^n)$ has exactly one subfield with p^m elements.

3. Let P_3 be the vector space of all polynomials over the real field \mathbb{R} of degree ≤ 3 . Define a mapping $\phi : P_3 \rightarrow \mathbb{R}$ by $\phi(a_0 + a_1x + a_2x^2 + a_3x^3) = a_0 + a_1 + a_2 + a_3$ for every $a_0 + a_1x + a_2x^2 + a_3x^3 \in P_3$.
 - (a) Prove: $\phi \in P_3^*$, the dual space of P_3 (by definition, the dual space of a real vector space is the space of all linear functions from the space to \mathbb{R}).
 - (b) Let $\phi_0, \phi_1, \phi_2, \phi_3$ be the basis of P_3^* which is dual to the basis $\{1, x, x^2, x^3\}$, i.e., $\phi_j(x^i) = 0$ if $i \neq j$ and $\phi_i(x^i) = 1$, for $i = 0, 1, 2, 3$. Express the linear function ϕ of part (a) in terms of this dual basis.

1. (a) What is meant by the statement that a field is a normal extension of the rational field \mathbb{Q} ?
(b) Let $K = \mathbb{Q}(2^{1/2}, 2^{1/3})$. Determine the relative degree $[K : \mathbb{Q}]$.
(b) Prove that K is not a normal extension of \mathbb{Q} .

2. (a) State any one of Sylow's Theorems on finite groups. Consider the set of nonsingular matrices $\begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix}$ with elements α, β in the field with 3 elements.
(b) Prove that they form a group under multiplication.
(c) Determine the structure of this group, in particular whether it is abelian.

3. Let K be an arbitrary field and $K(x)$ the field of rational functions in one variable over K . Let u be an element of $K(x)$ not in K . Show:
(a) u is not algebraic over K .
(b) If $u = f(x)/g(x)$ where $f(x)$ and $g(x)$ are relatively prime polynomials in $K[x]$ then $[K(x) : K(u)] = m$ where $m = \max\{\deg f(x), \deg g(x)\}$.

4. Let \mathbb{Q} be the rational field and let α be a root of $x^4 + 1$. Show:
(a) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
(b) $\mathbb{Q}(\alpha)$ is a Galois extension of \mathbb{Q} .
(c) The Galois group of $\mathbb{Q}(\alpha)$ over \mathbb{Q} is the Klein 4-group.

1. (a) Consider a group G of order $2n$ which contains exactly n elements of order 2. Show that n must be odd.
(b) Let $A = \{a_1, \dots, a_n\}$ be the set of those elements of G which are of order 2. Prove that $a_i a_j \neq a_j a_i$ for all $i \neq j$.
(c) Give an example of a group of the type given in part (a).

2. (a) Let G be a finite group, H a normal subgroup, p a prime, $p \nmid [G : H]$. Show that H contains every Sylow p -subgroup of G .
(b) Show that a group of order 992 ($= 31 \cdot 32$) is not simple.

3. Let R be a commutative ring with 1, and let I, J be ideals in R with $I + J = R$.
(a) Let $a, b \in R$. Prove that there exists $c \in R$ such that $c \equiv a \pmod{I}$ and $c \equiv b \pmod{J}$.
(b) Deduce from the above that $R/I \cap J$ is isomorphic to the direct product $(R/I) \times (R/J)$.
[Note: You may do part (b) for partial credit, assuming the result for part (a), even if you haven't done part (a).]

4. Let R be a commutative ring with 1. Let f_1, f_2, \dots, f_r be r elements of R and let (f_1, \dots, f_r) be the ideal generated by this set. Suppose that g and h are elements of R and that a certain positive power of g belongs to (f_1, \dots, f_r, h) while a positive power of gh belongs to (f_1, \dots, f_r) . Show that there is a positive power of g which belongs to (f_1, \dots, f_r) .

SOLVING COMPLETELY ANY 4 OF THE PROBLEMS SECURES THE MAXIMUM SCORE OF 100 POINTS

1. Let $\omega = e^{2\pi i/5}$.

- (a) If possible, find a field $F \subset \mathbb{Q}(\omega)$ such that $[F(\omega) : F] = 2$.
- (b) If possible, find a field $F \subset \mathbb{Q}(\omega)$ such that $[F(\omega) : F] = 3$.

2. If p is a prime, let \mathbb{F}_p denote the finite field with p elements. Find the Galois group of $x^4 - 3$ over each of the following fields:

- (a) \mathbb{F}_7 .
- (b) \mathbb{F}_{13} .

3. Let G be a finite group with nm elements and K a *subset* with m elements. Define a “coset” of K to be $Kg = \{kg : k \in K\}$ where g is an element chosen from G .

Suppose that there exist exactly n distinct cosets of K in G . Prove that one of these “cosets” is a subgroup H and that the other “cosets” are then really the right cosets of the subgroup H in G .

4. (a) Show that a group of order 12 is not simple.
(b) Show that a group of order p^2q is not simple where p and q are distinct odd primes.
5. (a) Let B be a nontrivial Boolean ring (so $B \neq \{0\}$ and for all $b \in B$, $b^2 = b$). Prove:
(i) B is commutative.
(ii) If P is any prime ideal in B , then P is maximal.
(b) Let R be a noncommutative ring with multiplicative identity 1.
(i) Let $x \in R$ be arbitrary. If $r(x) = \{y \in R : xy = 0\}$, prove that $r(x)$ is a right ideal in R .

1. Let K be a field and $K[[x]]$ the ring of all formal power series with coefficients in K . Prove:

- (a) $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $K[[x]]$ if and only if $a_0 \neq 0$.
(b) $K[[x]]$ has only one maximal ideal.

2. Let R be a commutative ring with only one maximal ideal P . Let M be a finitely generated R -module for which $PM = M$. Prove that $M = 0$.

3. Prove: There is no simple group of order 36.

4. Prove: The order of $GL_n(\mathbb{F}_q)$ is $\prod_{j=0}^{n-1} (q^n - q^j)$.

5. Let k be a field and $k(x)$ the field of rational functions in one variable over k . Prove: $GL_2(k)/k^* = PGL_2(k)$ is the Galois group of $k(x)$ over k .

6. Let K be the fixed field of $PGL_2(\mathbb{F}_q)$ acting on $\mathbb{F}_q(x)$. Prove $K = \mathbb{F}_q(y)$ where $y = \frac{(x^{q^2} - x)^{q+1}}{(x^q - x)^{q^2+1}}$.

1. Let \mathbb{F}_q be a finite field with q elements. What is the number of quadratic (of exact degree 2) irreducible polynomials in $\mathbb{F}_q[x]$?

2. (a) Prove that the polynomial $x^4 - 3$ is irreducible over the field \mathbb{Q} of rational numbers.
(b) What is the degree of a splitting field K of $x^4 - 3$ over \mathbb{Q} ? Give a set of field generators for K over \mathbb{Q} . (Take K to be a subfield of the complex numbers.)
(c) Prove $x^4 - 3$ is irreducible over $\mathbb{Q}(i)$.
(d) Determine the Galois group of $x^4 - 3$ over $\mathbb{Q}(i)$ as an abstract group.

3. Let V be a vector space over a field K , R a subring of the ring $\text{Hom}(V)$ of linear transformations from V to V , and $\text{Hom}_R(V)$ the ring $\{S \in \text{Hom}(V) : ST = TS \text{ for all } T \in R\}$.
Prove: If R is 1-transitive, i.e., for all $x, y \in V$ with $x \neq 0$ there is a $T \in R$ with $T(x) = y$, then $\text{Hom}_R(V)$ is a division ring.

4. Let G be a finite group of order n . Assume that, for each prime dividing n , G has a unique Sylow p -subgroup P , and that P is cyclic. Prove that G is cyclic.

5. Let p, q, r be distinct primes.
(a) Show that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$.
(b) Show that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r}) : \mathbb{Q}] = 8$.

6. (a) Determine for which pairs k, n with $1 \leq k \leq n$ there is a $k \times k$ matrix A over the rationals \mathbb{Q} such that $A^n = 2I$.
(b) Give, with proof, an example, for each n , of a linear transformation $T : \mathbb{Q}^n \rightarrow \mathbb{Q}^n$ such that the only T -invariant subspaces of \mathbb{Q}^n are $\{0\}$ and \mathbb{Q}^n .

1. Let G be an arbitrary group whose center is trivial. Prove: The center of the automorphism group of G is also trivial.

2. Let L be a separable extension of degree n of the field K . Assume L is contained in a given algebraic closure \overline{K} of K . Let $\{v_1, \dots, v_n\}$ be a vector space basis for L over K . Let $v_i^{(j)}$, $j = 1, \dots, n$ be the conjugates of v_i in \overline{K} . Prove

$$\det \begin{pmatrix} \vdots & & \vdots \\ \dots\dots\dots & v_i^{(j)} & \dots\dots\dots \\ \vdots & & \vdots \\ \vdots & & \vdots \end{pmatrix} \neq 0.$$

3. Determine all maximal ideals in the polynomial ring $\mathbb{Z}[x]$. (\mathbb{Z} is the ring of rational integers.)

4. How many irreducible factors does the polynomial $x^{2^{10}-1} - 1$ have over $GF(2)$?

5. Let ω_1, ω_2 be two complex numbers whose ratio $\omega = \omega_1/\omega_2$ is not real. Let $\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ be the abelian group generated by ω_1 and ω_2 . Let $R = \{\lambda \in \mathbb{C} : \lambda\Lambda \subseteq \Lambda\}$ (\mathbb{C} is the field of complex numbers).

(a) Prove: R is a ring.

(b) Prove: If λ is a unit in R then λ is a root of unity. ($\lambda^n = 1$ for some $n > 0$.)

(c) If λ is an n^{th} root of unity in R then n is a divisor of ??.

6. Let R be a ring (associative with identity) for which $b^2 = b$ for every b in R . Let \mathfrak{p} be a prime ideal of R .

(a) Prove: R is commutative.

(b) Prove: R/\mathfrak{p} is a field.

1. An element r in a ring is called *nilpotent* if $r^n = 0$ for some positive integer n .
 - (a) Show that in a commutative ring R the set of nilpotent elements forms an ideal N .
 - (b) In the notation of (a) show that R/N has no nilpotent elements.
 - (c) Show by example that part (a) need not be true for noncommutative rings.

2. Let $F = \mathbb{Q}(\theta)$ where \mathbb{Q} denotes the rational number field and θ the fifth root of unity $e^{2\pi i/5}$. Discuss the Galois group of the polynomial $x^5 - 7$ over $\mathbb{Q}(\theta)$, including a determination of the degree of the root field (justify this), a description of the Galois group in purely group-theoretic language, and a representation of each automorphism as a permutation.

3. Either: Let G be a finite group of order $2p$, p and odd prime. Let a be an element of order 2, b an element of order p . Let H be the subgroup of G which is generated by b .
 - (i) Prove H is a normal subgroup of G .
 - (ii) Prove that $aba = b^r$ for some integer r , and hence that $b^{r^2} = b$.Deduce that one of the relations $aba = b$; $aba = b^{-1}$ must hold.

Or: State some theorem involving Sylow subgroups and use it to show that a group of order 30 cannot be simple.

4. $f_j(x)$, $j = 1, \dots, k$ ($k \geq 2$) are polynomials in x with complex coefficients. Assume that they have no common root; thus for any x

1. (a) Let G be a cyclic group of order n . Let $d \in \mathbb{Z}^+$, and let $\nu = \gcd(d, n)$. Show that n/ν of the elements of G are d^{th} powers (i.e., are of the form y^d for some $y \in G$).
(b) Let $d, s \in \mathbb{Z}^+$, and let $p \in \mathbb{Z}^+$ be an odd prime (so the group of units U of the ring $\mathbb{Z}/p^s\mathbb{Z}$ is cyclic). When is the d^{th} power mapping ($y \rightarrow y^d$) on U surjective?

2. Let G be the abelian, non-cyclic group of order 25. Let the field K be a Galois (finite, separable, normal) extension of the field F , with Galois group G .
 - (a) Find $[K : F]$, the degree of the field extension.
 - (b) How many intermediate fields Σ are there between F and K ? ($F \leq \Sigma \leq K$)
 - (c) Which of the above fields Σ are normal extensions of F ?

3. Let ω_1, ω_2 be a pair of complex numbers that are linearly independent over the reals. Let Λ be the free abelian group generated by ω_1, ω_2 . That is, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Now let $R = \{\lambda \in \mathbb{C} : \lambda\Lambda \leq \Lambda\}$. Show:
 - (a) R is a commutative ring containing \mathbb{Z} as a subring.
 - (b) $\mathbb{Z} \not\cong R \iff \omega = \omega_1/\omega_2$ generates a quadratic extension of \mathbb{Q} .
 - (c) Suppose that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ and $\omega^2 + r\omega + s = 0$ with suitable $r, s \in \mathbb{Q}$. Let $r = r_1/r_2$, $s = s_1/s_2$ where r_1, r_2, s_1, s_2 are integers and $\gcd(r_1, r_2) = \gcd(s_1, s_2) = 1$. Finally let $c = \text{lcm}(r_2, s_2)$. Prove $R = \mathbb{Z}[c\omega]$.

1. Let K be a field of degree n over the rational numbers, \mathbb{Q} . Moreover, let $\{w_1, \dots, w_n\}$ be a basis for K as a vector space over \mathbb{Q} . Next, when $\alpha \in K$ let $p_\alpha(x)$ be its minimal polynomial over \mathbb{Q} and $n_\alpha = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Since $\alpha K \subset K$ we can write $\alpha w_i = \sum_{j=1}^n a_{ji} w_j$, $i = 1, \dots, n$. Let

$$A_\alpha = \begin{pmatrix} & & & & \\ & & & & \vdots \\ & & & & a_{ji} \\ \cdots & & & & \vdots \\ & & & & \vdots \end{pmatrix}.$$

We define $\Phi : K \rightarrow M_n(\mathbb{Q})$ by $\Phi(\alpha) = A_\alpha$.

- Show that Φ is a monomorphism of the field K into the ring $M_n(\mathbb{Q})$.
- For a given $\alpha \in K$ what are the minimal and characteristic polynomials of A_α ? (Give these explicitly.)
- Compute the minimal and characteristic polynomials in the case: $K = \mathbb{Q}(i, \sqrt{2})$, $\alpha = i$, $w_1 = 1$, $w_2 = i$, $w_3 = \sqrt{2}$, $w_4 = i\sqrt{2}$. Also find $\Phi(\alpha)$ in this case.

2. Let $R = \mathbb{Z} \left[\frac{1+\sqrt{-11}}{2} \right]$ be the ring of all complex numbers of the form $m + n \left(\frac{1+\sqrt{-11}}{2} \right)$ where m and n are ordinary integers. When $a \in R$ we let $|a|$ be its length as a complex number.

- Show that R is a Euclidean ring. That is, show that for all $a, b \neq 0$ in R there exist q, r in R such that $a = bq + r$ and $|r| < |b|$.
- Since Euclidean rings are unique factorization domains, factor 37 into prime factors in R .

3. Let H be a subgroup of a group G . Let $N_G(H)$, $C_G(H)$ be, respectively, the normalizer and the centralizer of H , i.e., $N_G(H) = \{x \in G : x^{-1}Hx = H\}$, $C_G(H) = \{x \in G : xg = gx \text{ for all } g \in H\}$.

- Prove that $C_G(H)$ is a normal subgroup of $N_G(H)$, and that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of the automorphism group of H .
- A celebrated theorem (credited to Burnside) is: "Let the order of a finite group G be $p^\alpha m$, where p is a prime, and $(p, m) = 1$. Let P be a Sylow p -subgroup of G . Suppose $N_G(P) = C_G(P)$. Then G has a normal subgroup of order m ."

Use this theorem to prove the following: Let G be a finite group of order $p^\alpha m$, where p is the smallest prime dividing the order of G , and $(m, p) = 1$. Suppose P is cyclic, where P is a Sylow p -subgroup of G . Then G has a normal subgroup of order m .

4. Let K be a splitting field of $x^{12} - 1$ over \mathbb{Q} , where \mathbb{Q} is the field of rational numbers.

- Describe the Galois group of K over \mathbb{Q} (what are its elements and what is the group structure?).
- How many subfields does K have and what are their degrees over \mathbb{Q} ?
- Let θ be a primitive 12^{th} root of unity in an extension field of \mathbb{Q} (i.e., $\theta^{12} = 1$ and $\theta^m \neq 1$ if $0 < m < 12$). Find the irreducible polynomial for θ over \mathbb{Q} .

5. Let R be a ring with identity and M a unitary R -module.
- (a) If $m \in M$ show that $\{x \in R : xm = 0\}$ is a left ideal of R .
 - (b) Let A be a left ideal of R and $m \in M$. Show that $\{xm : x \in A\}$ is a submodule of M .
 - (c) Suppose it is given that M has no submodules other than $\{0\}$ and M itself (one says that M is *irreducible*). Let $m_0 \in M$, $m_0 \neq 0$. Show that $A = \{x : xm_0 = 0\}$ is a maximal left ideal of R (that is, if A is contained properly in a left ideal B , then $B = R$).
6. Let ω_1, ω_2 be a pair of complex numbers such that $\omega = \omega_1/\omega_2$ lies in the upper half plane (i.e., $\text{Im}(\omega) > 0$). Let $\Lambda = \{m\omega_1 + n\omega_2 \in \mathbb{C} : m, n \in \mathbb{Z}\}$. Let $E(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \leq \Lambda\}$. (Note: $\mathbb{Z} \leq E(\Lambda)$.)
- (a) Show: if $\mathbb{Z} \not\leq E(\Lambda)$ then $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.
 - (b) Show: If $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ then $\mathbb{Z} \not\leq E(\Lambda)$ and every $\alpha \in E(\Lambda)$ satisfies an integral equation (i.e., $\alpha^2 + a\alpha + b = 0$ for some a, b in \mathbb{Z}).
 - (c) Compute $E(\Lambda)$ explicitly in the case $\omega = \sqrt{-1}$. (Be careful of this one!)

1. Suppose R is a Boolean ring, i.e., a ring such that $x^2 = x$ for all $x \in R$.

(a) Prove that R is commutative and of characteristic 2.

From now on assume there is a unit element $1 \in R$. For $a \in R$, we let (a) denote the principal ideal generated by a .

(b) Prove that for $a \in R$, (a) is itself a Boolean ring with unit element a .

(c) Prove that, for any $a \in R$, the ring R is the direct sum of the ideals (a) , $(1 + a)$:

$$R = (a) \oplus (1 + a).$$

(d) Prove that any finite Boolean ring is isomorphic to a direct power of the two-element ring \mathbb{Z}_2 (a direct sum of several copies of \mathbb{Z}_2).

2. (a) A group G is *decomposable* if it is isomorphic to a direct product of two proper subgroups. Otherwise G is *indecomposable*.

Prove that a finite abelian group G is indecomposable if and only if G is cyclic of prime power order.

(b) Determine all positive integers n for which it is true that the only abelian groups of order n are the cyclic ones. Justify your answer.

3. Let S be the set of all 2×2 Hermitian matrices of trace 0, i.e., $\{A : \bar{A}^t = -A \text{ and } \text{tr}(A) = 0\}$ ($B^t =$ transpose of B).

(a) Prove that the mapping

$$(x, y, z) \rightarrow \begin{pmatrix} x & y + iz \\ y - iz & -x \end{pmatrix}$$

is an isomorphism of \mathbb{R}^3 onto S .

Let G be the set of all unitary 2×2 complex matrices, i.e., $\{A : A \cdot \bar{A}^t = \bar{A}^t \cdot A = I\}$. For each matrix $A \in G$ define $\varphi_A(B) = ABA^{-1}$ for any 2×2 complex matrix B .

(b) Prove that φ_A maps $S \rightarrow S$, and is a linear transformation of S into itself.

(c) Making use of the isomorphism in part (a), prove that the mapping $A \rightarrow \varphi_A$ is a group homomorphism of G onto a group of distance-preserving linear transformations of \mathbb{R}^3 .

4. (a) List, without proof, the standard results you know on finite fields (including their Galois theory).

For any prime p , let $\mathbb{F} = \mathbb{Z}_p$, the field with p elements. Let K be an algebraic closure of \mathbb{F} , and let G be the group of automorphisms of K .

You may use, in the following, any result quoted in part (a).

(b) Prove that for any positive integer n , K contains one and only one subfield with $q = p^n$ elements.

(c) Let E be any finite subfield of K , and let $\sigma \in G$. Prove $\sigma(E) = E$.

(d) Prove that G is an abelian group.

1. (a) Determine the splitting field K for the polynomial $x^4 - 5$ over \mathbb{Q} (the field of rational numbers) and give the degree $[K : \mathbb{Q}]$.
(b) Find a set of automorphisms of K which generate the Galois group of K over \mathbb{Q} (but do not list all the elements of the Galois group).
(c) What is the order of the Galois group G of K over \mathbb{Q} ?
(d) Give an example of intermediate fields $F_1, F_2 : \mathbb{Q} \subsetneq F_1 \subsetneq K, \mathbb{Q} \subsetneq F_2 \subsetneq K$ such that F_1 is normal over \mathbb{Q} and F_2 is not normal over \mathbb{Q} .
(e) Find the subgroups H_1 and H_2 of G which correspond to F_1 and F_2 , respectively, under the Galois correspondence.

2. If a matrix A has a minimal polynomial $(x - 3)^3(x - 5)^2(x - 2)$ and characteristic polynomial $(x - 3)^5(x - 5)^5(x - 2)$, give the possible Jordan canonical forms that might correspond to A .

3. Let R be a noncommutative ring with multiplicative identity 1.
(a) Let $x \in R$. If $r(x) = \{y \in R : xy = 0\}$ prove that $r(x)$ is a right ideal of R .
(b) Let x be an element of R which has a right multiplicative inverse z in R . Prove that z is also a left inverse of x if and only if $r(x) = 0$.
(c) Prove that if an element x of R has more than one right inverse then it has infinitely many.
[Hint: Note if $xz = 1$ and $a \in r(x)$ then $x(z + a) = 1$.

4. Prove the theorem: If G is a nonabelian group then $G/Z(G)$ is not cyclic (where $Z(G)$ denotes the center of the group G).

5. Let G be a group of order p^2q where p and q are distinct odd primes. Prove that G contains a normal Sylow subgroup.

1. Prove that all groups of order 45 are abelian, and determine how many nonisomorphic groups of order 45 there are.

2. Let p be an odd prime. For any positive integer n , call an integer, a , a *quadratic residue* mod p^n if $(a, p) = 1$ and the equation $x^2 = a$ is solvable mod p^n . Prove that for any n , the quadratic residues mod p^n are precisely the quadratic residues mod p . [Hint: Use the fact that the group of units of the ring \mathbb{Z}_{p^n} form a cyclic group of order $p^{n-1}(p-1)$.

3. Prove that the multiplicative group of an infinite field is never cyclic.

4. Let K be the splitting field of $(x^3 - 2)(x^2 - 2)$ over the rational numbers \mathbb{Q} . Determine all subfields of K which are of degree four over \mathbb{Q} . Explain how you know you have found them all.

5. Let A be a 4×4 matrix over the field F . Suppose that

- (i) $A \neq I$,
- (ii) $A - I$ is nilpotent, i.e., there exists a positive integer n such that $(A - I)^n = 0$, and
- (iii) A has finite multiplicative order, i.e., there exists a positive integer m such that $A^m = I$.

For what fields F does such a matrix A exist? Clearly indicate your reasoning.

6. Let T be a linear transformation of V into V , where V is a finite-dimensional vector space over the complex numbers. Let p be any polynomial with complex coefficients. Show $p(T)$ has exactly the eigenvalues $p(\lambda_1), \dots, p(\lambda_n)$ if $\lambda_1, \dots, \lambda_n$ are the eigenvalues of T .

1. Let $N : GF(q^n)^* \rightarrow GF(q)^*$ by $N(a) = a^{1+a+\cdots+a^{q^{n-1}}}$. Prove: N is onto.
2. Let V be an n -dimensional vector space over the field k . Let S be a set of pairwise commuting linear transformations of V into V . Prove: If each f in S can be represented by a diagonal matrix with respect to some basis of V (depending on f), then there is a basis of V with respect to which *all* of the endomorphisms in S are diagonal.
3. Prove: The group of units of the ring $\mathbb{Z}/p^n\mathbb{Z}$ is a cyclic group of order $(p-1)p^{n-1}$ when p is an odd rational prime. [Hint: Use induction on n .]
4. Let K be the splitting field of $x^7 - 3x^3 - 6x^2 + 3$ over \mathbb{Q} . Let E_1, E_2 be subfields of K such that $[K : E_1] = [K : E_2] = 7$. Prove $E_1 \cong E_2$.
5. Find the Galois group of the splitting field K of $x^4 - 2$ over \mathbb{Q} . Find two subfields E_1, E_2 of K such that $[K : E_1] = [K : E_2] = 2$ but E_1 and E_2 are not isomorphic.
6. Let K be a field in which -1 cannot be represented as a sum of squares and such that in every proper algebraic extension -1 can be represented as a sum of squares. Prove: If $a \in K$ is not a square in K then a is not a sum of squares in K .

PLEASE DO 5 OUT OF 6 PROBLEMS

1. Show that no real 3×3 matrix satisfies $x^2 + 1 = 0$. Show that there are complex 3×3 matrices which do. Show that there are real 2×2 matrices that satisfy the equation.

2. Prove: Let G be a finite group, let H be a subgroup of G . Let $i(H)$ be the index of H . Let $o(G)$ be the order of G . Suppose $o(G)$ does not divide $i(H)$. Then H must contain a nontrivial normal subgroup of G . In particular, G cannot be simple.

[Hint: Let S be the set of right cosets of H . Let $a, g \in G$. Let $\theta_a : Hg \rightarrow Hga$. θ_a is a one-to-one mapping of S . Consider the collection of $\{\theta_a : a \in G\}$.]

Use this theorem to show that a group of order 75 cannot be simple. You may use Sylow's theorem.

3. Let G be a group of order p^n , where p is a fixed prime and n is a positive integer. Prove:

- (a) The center of G is nontrivial, i.e., there is a $g \in G$, $g \neq 1$, $g \in$ center of G . The center of a group is $\{x \in G : xg = gx \text{ for all } g \in G\}$.
- (b) For every $m, m < n$, G has a subgroup of order p^m .
- (c) Every subgroup of order p^{n-1} is normal.

4. Let R be a unique factorization domain, and let K be its field of quotients. In the following we fix a prime element p in R .

- (a) Let $R_p = \{\frac{a}{b} \in K : a \in R, b \in R \text{ and } p \text{ does not divide } b \text{ in } R\}$. Prove R_p is a subring of K .
- (b) Find the units of R_p . What are the primes of R_p ? Prove R_p is a unique factorization domain.
- (c) Show that R_p has a unique maximal ideal.
- (d) Prove that R_p is a maximal subring of K , i.e., if S is a subring of K which contains R_p then $S = R_p$ or $S = K$.

5. Let R be a ring with more than one element and with the property that for each element $a \neq 0$ in R there exists a *unique* element b in R such that $aba = a$. Prove:

- (a) R has no nonzero divisors of zero.
- (b) $bab = b$.
- (c) R has a unity.
- (d) R is a division ring.

Note: If you can't do one part of this problem assume the result and go on to the next part.

6. Consider $p(x) = x^8 + 1$ as a polynomial over the rationals \mathbb{Q} . Let K be the splitting field of $p(x)$ over \mathbb{Q} . Find the Galois group G of $p(x)$, i.e., the group of automorphisms of K relative to \mathbb{Q} . Is this group abelian? If so, express it as a direct sum of cyclic groups. List all the subgroups of G .