ALGEBRA PRELIM — JANUARY 1996

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

   (a) Show that $G_L\mathrm{Aut}(G)$ (that is, the set $\{xy \ : \ x \in G_L, y \in \mathrm{Aut}(G)\}$) is a group of transformations of G. $G_L\mathrm{Aut}(G)$ is called the *holomorph* of G and is denoted $\mathrm{Hol}\,(G)$.

   (b) Show $G_R \subset \mathrm{Hol}\,(G)$, where G_R is the group of right translates of G.

   (c) Show that if G is finite, then $|\mathrm{Hol}\,(G)| = |G||\mathrm{Aut}(G)|$.

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 $\mathbb{Q}$.

   (a) Find the four roots of $h(x)$ in $\mathbb{C}$.

   (b) Find an $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$.

   (c) Describe all elements of $G = \mathrm{Gal}(L/\mathbb{Q})$ as permutations of the roots of $h(x)$.

   (d) 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 $H = \mathrm{Gal}(L/M)$. Which of the extensions M are normal over $\mathbb{Q}$?

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

   (a) Show that, if $m \in M$, then $\{x \in R \ : \ xm = 0\}$ 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 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 $\mathbb{Z}/p\mathbb{Z}$.

   (a) Show that $g(x)$ has no repeated roots in a splitting field extension.

   (b) Show that $g(x)$ has no roots in $\mathbb{Z}/p\mathbb{Z}$.

   (c) 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 $g(x)$.

   (d) Show that $g(x)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$.

   (e) Consturct a splitting field extension L for $g(x)$ over $\mathbb{Z}/p\mathbb{Z}$.

   (f) Find the Galois group $\mathrm{Gal}(L/(\mathbb{Z}/p\mathbb{Z}))$. 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 $f : \mathbb{Z} \to \mathbb{C}$ 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

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

   (a) 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.

ALGEBRA PRELIM **JANUARY 1996**

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 $f \to f * \delta_M$ 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 $\{x \to hxk \ : \ h \in H, k \in K\}$ 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 $|HxK| = |H|[K : x^{-1}Hx \cap K] = |K|[H : x^{-1}Kx \cap H]$.

ALGEBRA PRELIM **AUGUST 1995**

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 $K(b - b') = L$.

ALGEBRA PRELIM — JANUARY 1995

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

   (a) 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.

   (b) If χ and g are in $\widehat{G}$ and G, respectively, then $\chi(g)$ is a root of unity.

   (c) For any x in $\widehat{G}$, $G/\ker(\chi)$ is cyclic.

   (d) 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.

   (a) Show $GL_2(k)$ is a group under matrix multiplication.

   (b) Show that order of $GL_2(k)$ is $r = (q^2 - q)(q^2 - 1)$.

   (c) 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.

   (a) Show that K is formally real if and only if -1 cannot be expressed as a sum of squares in K.

   (b) Show that if K is real, closed then every sum of squares in K is a square in K.

   (c) 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 $R = \{z \in \mathbb{C} \ : \ zL \leq L\}$ and suppose R contains a non-integer z. Show:

   (a) $\tau = \omega_1/\omega_2$ generates a quadratic extension of the rational numbers.

   (b) If the minimal polynomial for τ is of the form $\tau^2 - r\tau - s$ for suitable integers r and s, then $R = \mathbb{Z}[\tau]$.

ALGEBRA PRELIM

JANUARY 1995

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.)

ALGEBRA PRELIM **AUGUST 1994**

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 $\varphi_j \in S_n$ $(j = 1, \ldots, n)$ where $\varphi_j(i) = j + i$ and reflections $\psi_j \in S_n$ $(j = 1, \ldots, n)$ 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 $(j = 1, \ldots, n)$.

   (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 $\{1, \ldots, n\}$? (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 $\mathrm{Gal}(K_1/\mathbb{Q})$, $\mathrm{Gal}(K_2/\mathbb{Q})$, $\mathrm{Gal}(K_3/\mathbb{Q})$ and $\mathrm{Gal}(K_4/\mathbb{Z}_2)$.

   (a) Which of these groups are isomorphic?

   (b) If ζ is a primitive 9^{th} 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. p 511

   (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 $x^3 - x + 1$.

$\sqrt{D} = -4a^3 - 27b^2$

$= 4$

$= 1 \in \mathbb{F}_3$

$[L : \mathbb{F}_3] = 3$

ALGEBRA PRELIM **AUGUST 1993**

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 $U \cap V$.
   (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
   $c \oplus d = c + d + 1$ and
   $c * d = cd + c + d$ for all elements c, d in R (where the addition and multiplication of the right hand side of these relations are those of R).
   (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 $\phi : A \to A$ 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 $\mathbb{F}[x]$. Check 0 and 1 ≠ Quadratic
   (b) Let K be the splitting field of $f(x)$ over $\mathbb{F}$. How many members does K have? 16
   (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.

α
$\alpha+1$
α^2
α^2+1

$L = \{x \in K : \sigma^2(x) = x\}$
$\sigma^2(\alpha) = \alpha+1$
$\sigma^2(\alpha^2) = \alpha^2+1$
$\sigma^2(\alpha^2+\alpha) = \alpha^2+\alpha+1+\alpha = \alpha^2+\alpha$
$\sigma^2(\alpha^2+\alpha+1) = \alpha^2+\alpha+1$

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

ALGEBRA PRELIM — JANUARY 1993

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.

ALGEBRA PRELIM

AUGUST 1992

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

2. Let $\mathcal{B} = \{v_1, \ldots, v_m\}$ 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 $\mathbb{Q}$:

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

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

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

(a) Show that $V = V^{\perp} \oplus W$ for some subspace W which satisfies $W^{\perp} \cap W = \{0\}$.

(b) 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 $\langle w + w', w + w' \rangle$.]

(c) 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 $w' \in W'$.

(d) FACT: Induction on $r = \dim W$ and (c) may be used to show that $V = V^{\perp} \oplus \mathbb{Q}x_1 \oplus \cdots \oplus \mathbb{Q}x_r$, 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, ${}^t SAS = D$ 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.

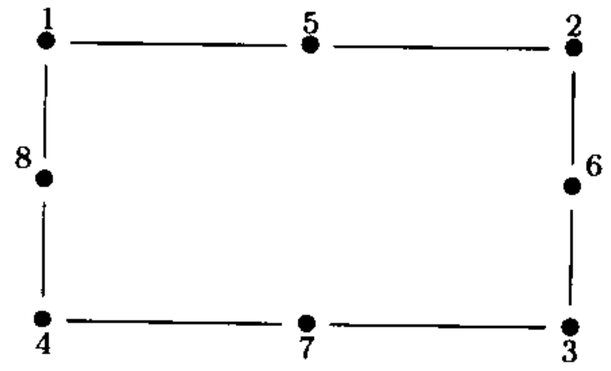
(a) Let m be the number of elements in the transitivity class (orbit) containing P. Show that $|G_P| m = N$ where $|G_P|$ denotes the order of the subgroup G_P.

(b) Suppose that P and Q are in the same transitivity class. Show that G_P and G_Q are isomorphic groups.

(c) 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

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

(d) 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 $\{1, 2, \ldots, 8\}$ to illustrate the theorem in part (c).



PLEASE TURN OVER

ALGEBRA PRELIM **AUGUST 1992**

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": $N(a + b\sqrt{-3}) = a^2 + 3b^2$.
   (a) What are the units in $\mathbb{Z}[\sqrt{-3}]$?
   (b) 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.
   (c) Test 5 and 7 to see if they are irreducible in $\mathbb{Z}[\sqrt{-3}]$.
   (d) 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 $\mathbb{Q}$.
   (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 $G = \mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order 6, and has as generator the map that takes $r \to r^3$ for any root r of $g(x)$.
   (c) Let ω be a complex 7^{th} root of 1. Let
   $$x_1 = \omega + \omega^2 + \omega^4, \qquad x_2 = \omega + \omega^6.$$
   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, 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 $\mathbb{Q}$.
   (a) Show that the four complex numbers $\pm\frac{\sqrt{2}}{2}(1 \pm i)$ are the four roots of $h(x)$ in $\mathbb{C}$.
   (a) Find an $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$.
   (c) Describe all elements of $G = \mathrm{Gal}(L/\mathbb{Q})$ as permutations of the roots of $h(x)$.
   (d) 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 $H = \mathrm{Gal}(L/M)$. Which of the extensions M are normal over $\mathbb{Q}$?

ALGEBRA PRELIM — JANUARY 1992

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 $i = 1, \ldots, n$, 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 $\phi(Av, Av) = 0$.

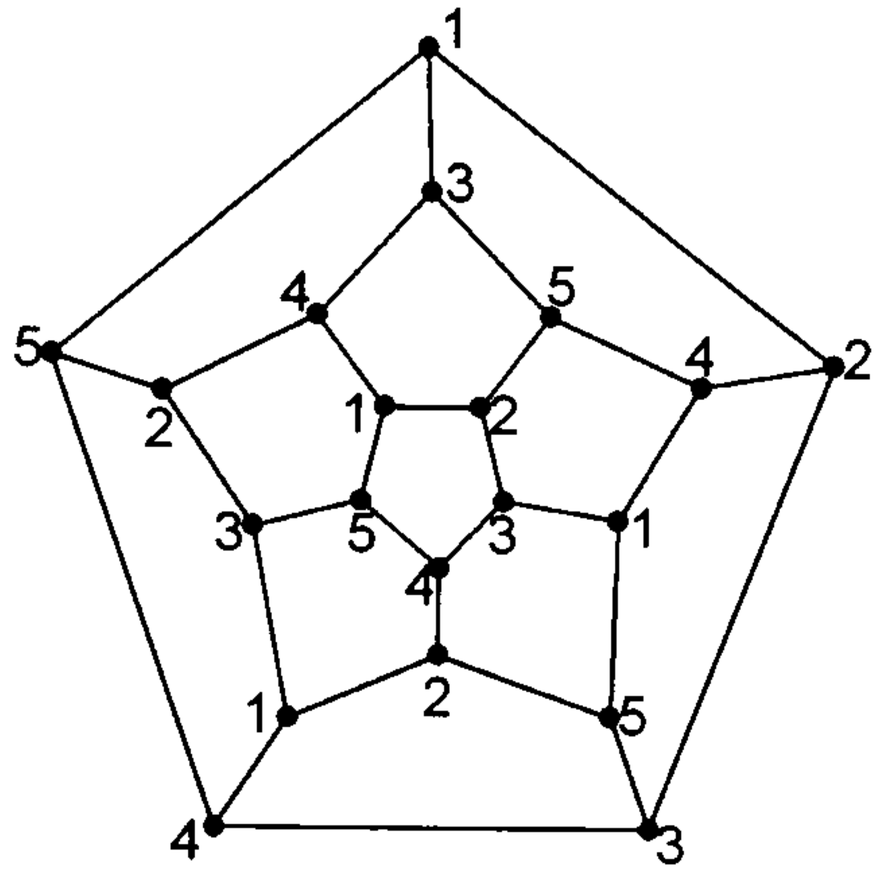
(iii) The columns c_i of A satisfy: $\phi(c_1, c_1) = \phi(c_2, c_2) = -\phi(c_3, c_3) = 1$ and $\phi(c_i, c_j) = 0$ for $i \neq j$.

(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.

ALGEBRA PRELIM **JANUARY 1992**

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

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

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:

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

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.

(a) Show that the order of G is $q^4 - q^3 - q^2 + q$.

(b) Let $H = \phi(G)$. Show that the order of H is $q^3 - q$.

(c) Use field theory to show that $f = \dfrac{(x^{q^2} - x)}{(x^q - x)}$ is relatively prime to $x^q - x$.

(d) 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.]

ALGEBRA PRELIM — AUGUST 1991

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 $f : R \to S$ with multiplicative identities 1_R and 1_S such that $f(1_R)$ does not equal 1_S.
   (b) If $f : R \to S$ is an epimorphism of rings with identity, show that $f(1_R) = 1_S$.
   (c) Now assume only that $f : R \to S$ 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.

ALGEBRA PRELIM — JANUARY 1991

DO 6 OF THE FOLLOWING 7 PROBLEMS

1. Let G be a group and $\mathrm{Aut}(G)$ 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 $\alpha \in \mathrm{Aut}(G)$. Now let

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

   (a) Show that B is a normal subgroup of $\mathrm{Aut}(G)$.
   (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

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

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

3. Let $G = \{a_1, \ldots, a_n\}$ 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

$$(p-1)! \equiv -1 \mod p.$$

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 $\mathbb{F}$.

ALGEBRA PRELIM

JANUARY 1991

6. Let $\mathbb{F}$ be a finite field with q elements and characteristic $p > 2$.
   (a) Show that exactly half the nonzero elments 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 $p \equiv 1 \mod 4$. (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

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

show that

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

PLEASE TURN OVER

ALGEBRA PRELIM

AUGUST 1990

PART II

4. Let $\mathbb{Z}_2$ denote the field with two elements.
   (a) If f is an irreducible polynomial of degree 17 over $\mathbb{Z}_2$, how many elements are there in the splitting field of f?
   (b) How many irreducible polynomials of degree 17 are there over $\mathbb{Z}_2$?

5. Let $R = \mathbb{Z}[x, y]$.
   (a) Prove or disprove: The ideal $I = (x, y)$ is a prime ideal in R.
   (b) Find all maximal ideals in R which contain I.
   (c) Prove or disprove: The ideal $J = (y^2 - x^3)$ is a prime ideal in R.

6. (a) Let $\phi : V \to V$ 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 $\phi : V \to V$ 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.
   (a) Find the degree of E over $\mathbb{Q}$.
   (b) 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 $f : F \to V \cup \{0\}$ with the following properties:
   (i) $f(0) = 0$ and $f(\alpha) > 0$ if $\alpha \neq 0$.
   (ii) $f(\alpha\beta) = f(\alpha)f(\beta)$ for all $\alpha, \beta \in F$.
   (iii) $f(\alpha + \beta) \leq \max\{f(\alpha), f(\beta)\}$.

   (a) Suppose F is an isosceles field. Let $R = \{\alpha \in F \ : \ f(\alpha) \leq 1\}$. Show that R is a ring with identity.
   (b) Let $P = \{\alpha \in F \ : \ f(\alpha) < 1\}$. Prove that P is a prime ideal of R.
   (c) 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 $\alpha_x : G \to G$, $\alpha_x(g) = x^{-1}gx$ 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

$$M_1 = \{em \ : \ m \in M\}, \qquad M_2 = \{(1-e)m \ : \ m \in M\}.$$

   (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.

ALGEBRA PRELIM

JANUARY 1990

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 $\mathrm{Gal}(K/\mathbb{Q})$ 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

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

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

$$(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times/S \simeq \{\pm 1\}$$

$$\chi$$

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

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

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

ALGEBRA PRELIM **AUGUST 1989**

1. Let k be an arbitrary field and let $k(z)$ be the field of rational functions in one variable over k. Let $a_1, \ldots, a_n$ be distinct elements of k. Let $e_1, \ldots, e_n$ 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 $a_1, \ldots, a_n$ and have multiplicities *at most* $e_1, \ldots, e_n$, 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 $\dim_k L = e_1 + \cdots e_n + 1$.
   (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 $[L : \mathbb{Q}]$.

ALGEBRA PRELIM **JANUARY 1989**

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 $T : GF(q) \to GF(p)$ be the trace map (i.e., $T(x)$ equals the sum of the conjugates of x). Let $\Phi : GF(q) \to GF(q)$ 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).

ALGEBRA PRELIM **AUGUST 1988**

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 mutiplicative 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.

ALGEBRA PRELIM **JANUARY 1988**

1. Determine up to isomorphism all groups of order 8.

2. Let G be a finite group and $f : G \to G$ 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.

ALGEBRA PRELIM **JANUARY 1987**

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 $\mathbb{Q}(\omega)$.