ALGEBRA PRELIM **JANUARY 1986**

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 $[E : F] = n =$ (degree of E 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 $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(f/\mathbb{Q})$ and all of its subgroups.

ALGEBRA PRELIM **AUGUST 1984**

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 or 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 $K = F(\beta)$. (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:

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

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 $\alpha < \beta < \gamma$.

ALGEBRA PRELIM **AUGUST 1983**

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 $\phi : P_3 \to \mathbb{R}$ 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.

ALGEBRA PRELIM **JANUARY 1983**

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.

ALGEBRA PRELIM **JANUARY 1982**

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 $A = \{a_1, \ldots, a_n\}$ 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 $c \equiv a \mod I$ and $c \equiv b \mod J$.
   (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 $f_1, f_2, \ldots, f_r$ be r elements of R and let $(f_1, \ldots, f_r)$ 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 $(f_1, \ldots, f_r, h)$ while a positive power of gh belongs to $(f_1, \ldots, f_r)$. Show that there is a positive power of g which belongs to $(f_1, \ldots, f_r)$.

ALGEBRA PRELIM **JANUARY 1981**

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.

ALGEBRA PRELIM **AUGUST 1980**

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

ALGEBRA PRELIM **JANUARY 1980**

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 $\mathrm{Hom}(V)$ of linear transformations from V to V, and $\mathrm{Hom}_R(V)$ the ring $\{S \in \mathrm{Hom}(V) \ : \ ST = TS \text{ for all } T \in R\}$.
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 $\mathrm{Hom}_R(V)$ 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 $T : \mathbb{Q}^n \to \mathbb{Q}^n$ such that the only T-invariant subspaces of $\mathbb{Q}^n$ are $\{0\}$ and $\mathbb{Q}^n$.

ALGEBRA PRELIM **JANUARY 1979**

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 $\{v_1, \ldots, v_n\}$ be a vector space basis for L over K. Let $v_i^{(j)}$, $j = 1, \ldots, n$ be the conjugates of v_i in $\overline{K}$. Prove

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

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.

ALGEBRA PRELIM **AUGUST 1978**

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

ALGEBRA PRELIM JANUARY 1978

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 $(y \to y^d)$ 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) $\mathbb{Z} \lneqq R \iff \omega = \omega_1/\omega_2$ 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 $c = \operatorname{lcm}(r_2, s_2)$. Prove $R = \mathbb{Z}[c\omega]$.

ALGEBRA PRELIM **JANUARY 1977**

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

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

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

(a) Show that Φ is a monomorphism of the field K into the ring $M_n(\mathbb{Q})$.

(b) For a given $\alpha \in K$ what are the minimal and characteristic polynomials of A_α? (Give these explicitly.)

(c) 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.

(a) 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 $|r| < |b|$.

(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., $N_G(H) = \{x \in G : x^{-1}Hx = H\}$, $C_G(H) = \{x \in G : xg = gx \text{ for all } g \in G\}$.

(a) 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.

(b) 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.

(a) Describe the Galois group of K over $\mathbb{Q}$ (what are its elements and what is the group structure?).

(b) How many subfields does K have and what are their degrees over $\mathbb{Q}$?

(c) 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 $\mathbb{Q}$.

PLEASE TURN OVER

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., $\mathrm{Im}\,(\omega) > 0$). 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 $\mathbb{Z} \lneqq E(\Lambda)$ then $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.
   (b) Show: If $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ then $\mathbb{Z} \lneqq E(\Lambda)$ 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!)

ALGEBRA PRELIM **AUGUST 1976**

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., $\{A \ : \ \overline{A}^t \text{ and } \operatorname{tr}(A) = 0\}$ (B^t = transpose of B).
   (a) Prove that the mapping
   $$(x, y, z) \to \begin{pmatrix} x & y + iz \\ y - iz & -x \end{pmatrix}$$
   is an isomorphism of $\mathbb{R}^3$ onto S.

   Let G be the set of all unitary 2×2 complex matrices, i.e., $\{A \ : \ A \cdot \overline{A}^t = \overline{A}^t \cdot A = I\}$. 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 $S \to S$, and is a linear transformation of S into itself.
   (c) Making use of the isomorphism in part (a), prove that the mapping $A \to \varphi_A$ 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.

ALGEBRA PRELIM JANUARY 1975

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.

ALGEBRA PRELIM

JANUARY 1974

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.

ALGEBRA PRELIM **AUGUST 1973**

1. Let $N : GF(q^n)^* \to GF(q)^*$ 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.

ALGEBRA PRELIM **JANUARY 1973**

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 $\theta_a : Hg \to Hga$. 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.