ALGEBRA PRELIM **JANUARY 2006**

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 $\mathrm{Aut}(G)$ 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 $\mathrm{Hom}_k(V, W)$ be the set of k-linear maps (= k-linear transformations) from V to W and let $V^* = \mathrm{Hom}_k(V, k)$.

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

ALGEBRA PRELIM AUGUST 2005

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 $S = R[x_1, \ldots, x_m]$ 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 $p_1, \ldots, p_n$ 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 $[E : \mathbb{Q}] = 2$.

ALGEBRA PRELIM JANUARY 2005

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.

ALGEBRA PRELIM

AUGUST 2004

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

2. Let p and q be distinct prime numbers with $p \not\equiv 1 \mod q$, and $q \not\equiv 1 \mod p$. 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 $\mathbb{Q}(z + 1/z)$.

ALGEBRA PRELIM **JANUARY 2004**

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 $SU(2) = \{g = (g_{ij})_{2\times 2} \ : \ g_{ij} \in \mathbb{C}, {}^t\overline{g}g = g\,{}^t\overline{g} = I_2, \det g = 1\}$; it is the special unitary group. An element $g \in SU(2)$ acts on H by $\rho(g) : x \in H \mapsto gx\,{}^t\overline{g} \in H$.
   (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 $SO(3) = \{q = (q_{ij})_{3\times 3} \ : \ q_{ij} \in \mathbb{R}, {}^tq\,q = q\,{}^tq = I_3, \det q = 1\}$.
   (b) Show that $\rho : SU(2) \to SO(3)$ is a homomorphism.
   (c) Find the kernel of $\rho : SU(2) \to SO(3)$.
   (d) Show that $\rho : SU(2) \to SO(3)$ 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 $\mathrm{End}_R(M) \cong \mathrm{End}_R(M_1) \oplus \mathrm{End}_R(M_2)$ as rings.
   (b) Now suppose $1 = e_1 + \cdots + e_n$, where e_i $(1 \le i \le n)$ are elements in the center of R and they are orthogonal idempotents, that is, they satisfy $e_i^2 = e_i$ (for all $1 \le i \le n$) and $e_ie_j = 0$ (for all $1 \le i \neq j \le n$). State and prove a generalization of the above result.
   (c) Let $R = \mathbb{C}[\mathbb{Z}_5]$ be the group algebra[1] 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.

[1]The 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

ALGEBRA PRELIM — AUGUST 2003

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

   (a) Show that $\mathrm{Hol}\, G$ is a group under composition and that if G is finite, then $|\mathrm{Hol}\, G| = |G| \times |\mathrm{Aut}(G)|$.

   (b) Prove that $\mathrm{Hol}\,(\mathbb{Z}_2 \times \mathbb{Z}_2)$ 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 $\phi : R \to R/I_1 \times R/I_2$ 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 $T : V \to V$ be a linear transformation from V to itself. Define a mapping $T^* : V^* \to V^*$ by $T^*(f) = f \circ T$.

   (a) Show that T^* is a linear transformation.

   (b) Let $B = \{e_1, \ldots, e_n\}$ be a basis for V and let $B^* = \{e_1^*, \ldots, e_n^*\}$ 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 $\mathbb{F}$.

   → [illegible] group of [illegible] field is cyclic [illegible]

   cyclic

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 $|\mathrm{Gal}(L/\mathbb{Z}_p)|$.

ALGEBRA PRELIM **JANUARY 2003**

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 an unique factorization domain that is not a principle 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 $T : V \to W$ a linear transformation. Let $\{w_1, w_2, \ldots, w_r\}$ be a basis for $T(V)$, and take $v_1, \ldots, v_r \in V$ such that $T(v_j) = w_j$ $(1 \le j \le r)$. Show that $v_1, \ldots, v_r$ are linearly independent. Then, let U be the space spanned by $v_1, \ldots, v_r$, and $K = \ker T$. Prove the theorem that states $rank(T) + nullity(T) = \dim(V)$ 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 $\{v_1, \ldots, v_m\}$ of V can be extended to a basis $\{v_1, \ldots, v_n\}$ 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 $\mathrm{Gal}(L/\mathbb{Q})$ 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 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$.
   (d) Find all intermediate fields M between L and $\mathbb{Q}$; for each such field M find a subgroup H of $\mathrm{Gal}(L/\mathbb{Q})$ such that $M = \mathrm{Fix}(H)$ and $H = \mathrm{Gal}(L/M)$. Which of the extensions $M : \mathbb{Q}$ are normal?

ALGEBRA PRELIM **AUGUST 2002**

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
$$\left(h(g)\right)^3 = 1$$
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
$$\left(t(A)\right)^3 = 1$$
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 $i = 1, \ldots, r$, $M_{i-1}/M_i \simeq A/P_i$ 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
$$\sum_{i=1}^{n} (-1)^i L_A(M_i) = 0.$$

PLEASE TURN OVER

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 $\mathbb{F}_2$.

ALGEBRA PRELIM JANUARY 2002

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 $\theta : H \to \mathrm{Aut}(G)$ a homomorphism. Let $G \times_\theta H$ be the set $G \times H$ with the following binary operation: $(g, h)(g', h') = \big(g[\theta(h)(g')], hh'\big)$.
   (a) Show that $G \times_\theta H$ is a group with the identity element (e, e') and $(g, h)^{-1} = \big(\theta(h^{-1})(g^{-1}), h^{-1}\big)$. (You may assume without proving it that the operation is associative.)
   13 (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 $a^5 = e$, $b^3 = e$, $c^7 = e$, $ab = ba$, $bc = cb$, $ac = ca$.
   (c) In the group described in (b), determine the number of Sylow subgroups.

3. (a) Suppose $0 \to A' \to A \to A'' \to 0$ is a short exact sequence of abelian groups. Show that $\operatorname{rank} A$ is finite if and only if $\operatorname{rank} A'$ and $\operatorname{rank} A''$ are finite. If so, show that $\operatorname{rank} A = \operatorname{rank} A' + \operatorname{rank} A''$.
   (b) Suppose $0 \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} \cdots \longrightarrow C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0 \longrightarrow 0$ is a chain of abelian groups, i.e., C_i is an abelian group and $d_i : C_i \longrightarrow C_{i-1}$ is a homomorphism such that $d_{i-1} \circ d_i = 0$, for each i. Let $H_i = \dfrac{\ker d_i}{\operatorname{Im} d_{i+1}}$ $(i = 0, 1, \ldots, n)$. Assume that $\operatorname{rank} C_i$ is finite, for all i. Define two polynomials
$$m(t) = \sum_{i=0}^{n} \operatorname{rank} C_i t^i, \qquad p(t) = \sum_{i=1}^{n} \operatorname{rank} H_i t^i.$$
   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 $\mathrm{Ann}(r) = \{m \in M \ : \ rm = 0\}$ 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.

ALGEBRA PRELIM **AUGUST 2000**

1. Determine the Galois groups of the following polynomials in $\mathbb{Q}[x]$:
   (a) $x^4 - 7x + 10$. → K lu
   (b) $x^3 - 2$. → S_3
   (c) $x^5 - 9x + 3$.
   p. 610

4.3 prop 10

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 $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ 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 $[\mathbb{Z}_2(\varphi) : \mathbb{Z}_2] = 2$.

ALGEBRA PRELIM **JANUARY 1999**

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, $R = S[x_1, \ldots, x_n]$. Let I be the ideal of R generated by the quadratic monomials $\{x_i x_j \ : \ 1 \le i, j \le n\}$, and ϕ the natural projection

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

   (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 $f' = \phi(f) - \phi(f(0, \ldots, 0))$. 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 $[\mathbb{Q}(r + 1/r) : \mathbb{Q}] \le 3$.
   (b) Deduce from (a) that the Galois group of f is solvable. [Hint: All groups of order less than 60 are solvable.]

ALGEBRA PRELIM **JANUARY 1998**

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 $\mathrm{Aut}(F(t)/F) \cong GL_2(F)/\{\lambda I \ : \ \lambda \in F^{\times}\}$, 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 $\mathrm{Aut}(\mathbb{F}_2(t)/\mathbb{F}_2) \cong S_3$.
   (c) Find the subfields of $\mathbb{F}_2(t)$ which are the fixed fields of the subgroups of $\mathrm{Aut}(\mathbb{F}_2(t)/\mathbb{F}_2)$.

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

Galois grp is S_5 p.610

PLEASE TURN OVER

6. An *ultrafilter* on $\mathbb{N} = \{0, 1, 2, \ldots\}$ 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.

ALGEBRA PRELIM **AUGUST 1997**

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 $f : V \to V$ 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 $N\left(m + n\frac{1+\sqrt{-11}}{2}\right) = \frac{(2m+n)^2 + 11n^2}{4}$.

ALGEBRA PRELIM JANUARY 1997

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 $\{1, 2, 3, \ldots, n\}$. Suppose that G is a subgroup of S_n of 2-power order. Prove that there exists $i \in \{1, 2, 3, \ldots, n\}$ 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 $T : V \to V$ 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 $G = \mathrm{Gal}(K/\mathbb{Q})$ 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 7^{th} 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.)

ALGEBRA PRELIM **AUGUST 1996**

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.

roots of $x^2 - \zeta_{12}$

ζ_{24}, ζ_{24}^{13}

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?

$(x^2 - \zeta_{12})(x^2 - \zeta_{12}^5)(x^2 - \zeta_{12}^7)(x^2 - \zeta_{12}^{11})$

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

$$N : \mathbb{F}_{q^r}^\times \to \mathbb{F}_q^\times$$

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.)