2018 Algebra Prelim

September 10, 2018

INSTRUCTIONS: Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it. Please start each solution on a new page and submit your solutions in order.

1. Show that no finite group is the union of conjugates of a proper subgroup.

2. Classify all groups of order 18 up to isomorphism.

3. Let α, β denote the unique positive real 5th root of 7 and 4th root of 5, respectively. Determine the degree of $\mathbb{Q}[\alpha, \beta]$ over $\mathbb{Q}$.

4. Show that the field extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2+\sqrt{2}}]$ is Galois and determine its Galois group.

5. Let M be a square matrix over a field K. Use a suitable canonical form to show that M is similar to its transpose M^T.

6. Let R be a commutative ring and M be an R-module.

(a) Show that $M = 0$ if and only if the localization $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of R.

(b) Find an example of a local ring R with maximal ideal $\mathfrak{m}$ and a nonzero R-module M such that $M/\mathfrak{m}M = 0$.

7. Let G be a finite group and π, π' be two irreducible representations of G. Prove or disprove the following assertion: π and π' are equivalent if and only if $\det \pi(g) = \det \pi'(g)$ for all $g \in G$.

8. Let K be a field and $R = K[x]/(x^2)$. For each integer $i \geq 0$, compute

(a) $\mathrm{Ext}^i_R(R, R/(x))$

(b) $\mathrm{Ext}^i_R(R/(x), R)$

(c) $\mathrm{Ext}^i_R(R/(x), R/(x))$.

Algebra prelim 2017

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Let R be a Noetherian ring. Prove that $R[x]$ and $R[\![x]\!]$ are both Noetherian. (The first part of the question is asking you to prove the Hilbert Basis Theorem, not to use it!)

2. Classify (with proof) all fields with finitely many elements.

3. Suppose A is a commutative ring and M is a finitely presented module. Given any surjection $\phi : A^n \to M$ from a finite free A-module, show that $\ker(\phi)$ is finitely generated.

4. Classify all groups of order 57.

5. Let H_n denote the Heisenberg group of order n^3, i.e.,

$$H_n \;=\; \langle a, b, c \mid a^n = b^n = c^n = 1,\, ba = cab, c \text{ is central}\rangle.$$

   (a) Show that

$$H_n \;\cong\; \left\{ \begin{pmatrix} 1 & u & w \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; u, v, w \in \mathbb{Z}/n\mathbb{Z} \right\}$$

   (b) Classify the irreducible complex representations of H_p when p is prime.

6. Find all ring homomorphisms $\mathbb{Q}[x]/(x^{100}+2) \to \mathbb{Q}[x]/(x^{1001}+2)$.

7. Show that a finite simple group can not have a 2-dimensional irreducible representation over $\mathbb{C}$. (Hint: the determinant might prove useful.)

8. If q is a power of a prime let $\mathbb{F}_q$ denote the field with q elements. Given an explicit description of $M_2(\mathbb{F}_4) \otimes_{\mathbb{F}_2} M_2(\mathbb{F}_4)$ as a direct product of matrix rings over division rings.

ALGEBRA PRELIMINARY EXAM – AUTUMN 2016

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count for more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Let G be a finite simple group (that is, a group with no proper nontrivial normal subgroup). Assume that every proper subgroup of G is abelian. Prove that then G is cyclic of prime order.

2. Let $a \in \mathbb{N}$, $a > 0$. Compute the Galois group of the splitting field of the polynomial $x^5 - 5a^4x + a$ over $\mathbb{Q}$.

3. Let $\mathfrak{m} \subset \mathbb{Z}[x_1, \ldots, x_n]$ be a maximal ideal. Show that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite field.

4. Recall that an inner automorphism of a group is an automorphism given by conjugation by an element of the group. An outer automorphism is an automorphism that is not inner.

(a) Prove that S_5 has a subgroup of order 20.

(b) Use the subgroup from (a) to construct a degree 6 permutation representation of S_5 (i.e., an embedding $S_5 \hookrightarrow S_6$ as a transitive permutation group on 6 letters).

(c) Conclude that S_6 has an outer automorphism.

5. Let A be a commutative ring and M a finitely generated A-module. Define

$$\mathrm{Ann}(M) = \{a \in A \mid am = 0 \text{ for all } m \in M\}.$$

Show that for a prime ideal $\mathfrak{p} \subset A$, the following are equivalent:

(a) $\mathrm{Ann}\, M \not\subset \mathfrak{p}$.

(b) The localization of M at the prime ideal $\mathfrak{p}$ is 0.

(c) $M \otimes_A k(\mathfrak{p}) = 0$, where $k(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is the residue field of A at $\mathfrak{p}$.

6. Let $A = \mathbb{C}[x, y]/(y^2 - (x-1)^3 - (x-1)^2)$.

(a) Show that A is an integral domain and sketch the $\mathbb{R}$-points of $\mathrm{Spec}\, A$.

(b) Find the integral closure of A. Recall that for an integral domain A with a fraction field K, the integral closure of A in K is the set of all elements of K integral over A.

7. Let $R = k[x, y]$ where k is a field, and let $I = (x, y)R$.

(a) Show that

$$0 \longrightarrow R \xrightarrow{\phi} R \oplus R \xrightarrow{\psi} R \longrightarrow k \longrightarrow 0$$

where $\phi(a) = (-ya, xa)$, $\psi((a, b)) = xa + yb$ for $a, b \in R$, is a projective resolution of the R-module $k \simeq R/I$.

(b) Show that I is not a flat R-module by computing $\mathrm{Tor}_i^R(I, k)$.

8. Let k be a field of positive characteristic p, $\mathbb{Z}/p$ a cyclic group of order p, and $k\mathbb{Z}/p$ the group algebra of $\mathbb{Z}/p$ over k.

(a) Let σ be a generator of $\mathbb{Z}/p$ and let $t = \sigma - 1$. Show that there is an isomorphism $k\mathbb{Z}/p \simeq k[t]/t^p$.

(b) Let M be a finite dimensional *projective* $k\mathbb{Z}/p$-module and Σ the linear operator on M induced by the action of σ. Show that

(i) $\dim_k M$ is divisible by p; and

(ii) $\mathrm{rk}(\Sigma - \mathrm{Id}_M) = \dfrac{p-1}{p} \dim_k M$.

(c) Let M be a finite dimensional $k\mathbb{Z}/p$-module, and assume that

$$\mathrm{rk}(\Sigma - \mathrm{Id}_M) = \frac{p-1}{p} \dim_k M.$$

Prove that then M is projective.

2015 Algebra Prelim

September 14, 2015

INSTRUCTIONS: Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. (a) Find an irreducible polynomial of degree 5 over the field $\mathbb{Z}_2$ of two elements and use it to construct a field of order 32 as a quotient of the polynomial ring $\mathbb{Z}_2[x]$.

(b) Using the polynomial you found in part (a), find a 5×5 matrix M over $\mathbb{Z}_2$ of order 31, so that $M^{31} = I$ but $M \neq I$.

2. Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Justify your answer.

3. (a) Let R be a commutative ring with no nonzero nilpotent elements. Show that the only units in the polynomial ring $R[x]$ are the units of R, regarded as constant polynomials.

(b) Find all units in the polynomial ring $\mathbb{Z}_4[x]$.

4. Let p and q be two distinct primes. Prove that there is at most one non-abelian group of order pq (up to isomorphisms) and describe the pairs (p, q) such that there is no non-abelian group of order pq.

5. (a) Let L be a Galois extension of a field K of degree 4. What is the minimum number of subfields there could be strictly between K and L? What is the maximum number of such subfields? Give examples where these bounds are attained.

(b) How do these numbers change if we assume only that L is separable (but not necessarily Galois) over K?

6. Let R be a commutative algebra over $\mathbb{C}$. A derivation of R is a $\mathbb{C}$-linear map $D : R \to R$ such that (i) $D(1) = 0$, and (ii) $D(ab) = D(a)b + aD(b)$ for all $a, b \in R$.

(a) Describe all derivations of the polynomial ring $\mathbb{C}[x]$.

(b) Let A be the subring (or $\mathbb{C}$-subalgebra) of $\mathrm{End}_{\mathbb{C}}(\mathbb{C}[x])$ generated by all derivations of $\mathbb{C}[x]$ and the left multiplications by x. Prove that $\mathbb{C}[x]$ is a simple left A-module. Note that the inclusion $A \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}[x])$ defines a natural left A-module structure on $\mathbb{C}[x]$.

7. Let G be a non-abelian group of order p^3 with p a prime.

(a) Determine the order of the center Z of G.

(b) Determine the number of inequivalent complex 1-dimensional representations of G.

(c) Compute the dimensions of all the inequivalent irreducible representations of G and verify that the number of such representations equals the number of conjugacy classes of G.

8. Prove that every finitely generated projective module over a commutative noetherian local ring is free.

2014 Algebra Prelim

September 8, 2014

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count for more than several partial solutions. Always justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. (a) Let G be a group (not necessarily finite) that contains a subgroup of index n. Show that G contains a *normal* subgroup N such that $n \leq [G : N] \leq n!$.

   (b) Use part (a) to show that there is no simple group of order 36.

2. Let p be a prime, let $\mathbb{F}_p$ be the p-element field, and let $K = \mathbb{F}_p(t)$ be the field of rational functions in t with coefficients in $\mathbb{F}_p$. Consider the polynomial $f(X) = X^p - t \in K[X]$.

   (a) Show that f does not have a root in K.

   (b) Let E be the splitting field of f over K. Find the factorization of f over E.

   (c) Conclude that f is irreducible over K.

3. Recall that a ring A is called *graded* if it admits a direct sum decomposition $A = \oplus_{n=0}^{\infty} A_n$ as abelian groups, with the property that $A_i A_j \subseteq A_{i+j}$ for all $i, j \geq 0$.

   Prove that a graded commutative ring $A = \oplus_{n=0}^{\infty} A_n$ is Noetherian if and only if A_0 is Noetherian and A is finitely generated as an algebra over A_0.

4. Let R be a ring with the property that $a^2 = a$ for all $a \in R$.

   (a) Compute the Jacobson radical of R.

   (b) What is the characteristic of R?

   (c) Prove that R is commutative.

   (d) Prove that if R is finite, then R is isomorphic (as a ring) to $(\mathbb{Z}/2\mathbb{Z})^d$ for some d.

5. Let R be a commutative ring and let M be an R-module.

   (a) Let $x \in R$ be a nonzero divisor. Compute $\mathrm{Tor}_i^R(R/(x), M)$ for $i \geq 0$.

(b) Show that M is a *flat* R-module if and only if $\mathrm{Tor}_1^R(M, N) = 0$ for all R-modules N.

(c) Conclude that if R is a PID and M is a finitely generated R-module, then M is flat if and only if M is free.

6. Let $\overline{\mathbb{F}_p}$ denote the algebraic closure of $\mathbb{F}_p$. Show that the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ has no nontrivial finite subgroups.

7. Let C_p denote the cyclic group of prime order p.

   (a) Show that C_p has two irreducible representations over $\mathbb{Q}$ (up to isomorphism), one of dimension 1 and one of dimension $p-1$.

   (b) Let G be a finite group, and let $\rho : G \longrightarrow \mathrm{GL}_n(\mathbb{Q})$ be a representation of G over $\mathbb{Q}$. Let $\rho_{\mathbb{C}} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$ denote ρ followed by the inclusion $\mathrm{GL}_n(\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$. Thus $\rho_{\mathbb{C}}$ is a representation of G over $\mathbb{C}$, called the complexification of ρ. We say that an irreducible representation ρ of G is *absolutely irreducible* if its complexification remains irreducible over $\mathbb{C}$.

   Now suppose G is abelian and that every representation of G over $\mathbb{Q}$ is absolutely irreducible. Show that $G \cong (C_2)^k$ for some k (i.e., is a product of cyclic groups of order 2).

8. Let G be a finite group and $\mathbb{Z}[G]$ the integral group algebra. Let $\mathcal{Z}$ be the center of $\mathbb{Z}[G]$. For each conjugacy class $C \subset G$, let $P_C = \sum_{g \in C} g$.

   (a) Show that the elements P_C form a $\mathbb{Z}$-basis for $\mathcal{Z}$. Hence $\mathcal{Z} \cong \mathbb{Z}^d$ as an abelian group, where d is the number of conjugacy classes in G.

   (b) Show that if a ring R is isomorphic to $\mathbb{Z}^d$ as an abelian group, then every element in R satisfies a monic integral polynomial. (**Hint:** Let $\{v_1, \ldots, v_d\}$ be a basis of R and for a fixed non-zero $r \in R$, write $rv_i = \sum_j a_{ij} v_j$. Use the Hamilton-Cayley theorem.)

   (c) Let $\pi : G \longrightarrow \mathrm{GL}(V)$ be an irreducible representation of G (over $\mathbb{C}$). Show that $\pi(P_C)$ acts on V as multiplication by the scalar

   $$\frac{|C|\chi_\pi(C)}{\dim V},$$

   where $\chi_\pi(C)$ is the value of the character χ_π on any element of C.

   (d) Conclude that $|C|\chi_\pi(C)/\dim V$ is an algebraic integer.

Algebra Prelim 2013

INSTRUCTIONS: Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

Notation: $\mathbf{Q}$ is the field of rational numbers and $\mathbf{C}$ is the field of complex numbers.

Problem 1. Let $\mathbf{Q}^\times$ be the nonzero elements of $\mathbf{Q}$, a group under multiplication.

(a) Prove that the additive group of $\mathbf{Q}$ has no maximal proper subgroups.

(b) Is the same statement true for the multiplicative group $\mathbf{Q}^\times$?

Problem 2. Let V be a finite-dimensional vector space over a field F of characteristic 0. Let $B : V \times V \to F$ be a non-degenerate, skew-symmetric bilinear form. (In particular, we have $B(x, y) = -B(y, x)$ for all $x, y \in V$.) If U is a subset of V, let

$$U^\perp \;=\; \{v \in V \mid B(u, v) = 0 \text{ for all } u \in U\}.$$

(a) Let U be a subspace of V. Prove that $U^\perp$ is a subspace of V and that

$$\dim_F(U) + \dim_F(U^\perp) = \dim_F(V)\ .$$

(b) Prove that there exists a subspace W of V such that $W^\perp = W$.

Problem 3.

(a) Suppose that G is a finitely-generated group. Let n be a positive integer. Prove that G has only finitely many subgroups of index n.

(b) Let p be a prime number. If G is any finitely-generated abelian group, let $t_p(G)$ denote the number of subgroups of G of index p. Determine the possible values of $t_p(G)$ as G varies over all finitely-generated abelian groups.

Problem 4. Suppose that G is a finite group of order 2013. Prove that G has a normal subgroup N of index 3 and that N is a cyclic group. Furthermore, prove that the center of G has order divisible by 11. (You will need the factorization $2013 = 3 \cdot 11 \cdot 61$.)

Problem 5. Let V be a finite dimensional vector space over $\mathbf{C}$. Let $n = dim_{\mathbf{C}}(V)$. Let $T : V \to V$ be a linear map. Suppose that the following statement is true.

For every $c \in \mathbf{C}$, the subspace $\{ v \in V \mid T(v) = cv \}$ of V has dimension 0 or 1.

Prove that there exists a vector $w \in V$ such that $\{w,\ T(w),\ ....,\ T^{n-1}(w)\}$ is a linearly independent set.

Problem 6. This question concerns an extension K of $\mathbf{Q}$ such that $[K : \mathbf{Q}] = 8$. Assume that $K/\mathbf{Q}$ is Galois and let $G = \mathrm{Gal}(K/\mathbf{Q})$. Furthermore, assume that G is nonabelian.

(a) Prove that K has a unique subfield F such that $F/\mathbf{Q}$ is Galois and $[F : \mathbf{Q}] = 4$.

(b) Prove that F has the form $F = \mathbf{Q}(\sqrt{d_1},\ \sqrt{d_2})$, where d_1 and d_2 are nonzero integers.

(c) Suppose that G is the quaternionic group. Prove that d_1 and d_2 are positive integers.

Problem 7. Let $R = \mathbf{C}[x_1, ..., x_n]$ be the polynomial ring over $\mathbf{C}$ in n indeterminates $x_1, ..., x_n$. Let S_n be the n-th symmetric group. If $\sigma \in S_n$, then we can identify σ with the automorphism of R defined as follows: $\sigma(c) = c$ for all $c \in \mathbf{C}$, and $\sigma(x_i) = x_{\sigma(i)}$ for all i, $1 \leq i \leq n$. Suppose that G is any subgroup of S_n. Let

$$S = R^G = \{r \in R \mid \sigma(r) = r \text{ for all } \sigma \in G\} \quad .$$

Prove that S is a finitely-generated $\mathbf{C}$-algebra.

Problem 8. This question concerns the polynomial ring $R = \mathbf{Z}[x, y]$ and the ideal $I = (5, x^2 + 2)$ in R.

(a) Prove that I is a prime ideal of R and that R/I is a PID.

(b) Give an explicit example of a maximal ideal of R which contains I.
(Give a set of generators for such an ideal.)

(c) Show that there are infinitely many distinct maximal ideals in R which contain I.

Algebra Prelim

September 10, 2012

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Classify all groups of order 2012 up to isomorphism. (Hint: 503 is prime.)

2. For any positive integer n, let G_n be the group generated by a and b subject to the following three relations:
$$a^2 = 1, \quad b^2 = 1, \quad \text{and} \quad (ab)^n = 1.$$
   (a) Find the order of the group G_n.
   (b) Classify all irreducible complex representations of G_4 up to isomorphism.

3. Let R be a (commutative) principal ideal domain, let M and N be finitely generated free R-modules, and let $\varphi : M \to N$ be an R-module homomorphism.
   (a) Let K be the kernel of φ. Prove that K is a direct summand of M.
   (b) Let C be the image of φ. Show by example (specifying R, M, N and φ) that C need not be a direct summand of N.

4. Let G be an abelian group. Prove that the group ring $\mathbb{Z}[G]$ is noetherian if and only if G is finitely generated.

5. Let $M_3(\mathbb{R})$ be the 3×3-matrix algebra over the real numbers $\mathbb{R}$. For any $b \in \mathbb{R}$, let $B \in M_3(\mathbb{R})$ be the matrix $\begin{pmatrix} 1 & b & 0 \\ b & 1 & b \\ 0 & b & 1 \end{pmatrix}$. Find the set of numbers b so that the matrix equation $X^2 = B$ has at least one, and only finitely many, solutions in $M_3(\mathbb{R})$.

6. Determine the Galois groups of the following polynomials over $\mathbb{Q}$.
   (a) $f(x) = x^4 + 4x^2 + 1$
   (b) $f(x) = x^4 + 4x^2 - 5$

7. Prove that if A is a finite abelian group, then $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) \cong A$. (Here, $\mathrm{Ext}^1_{\mathbb{Z}}(-,-)$ is also sometimes written as $\mathrm{Ext}(-,-)$.)

8. Let A be the $\mathbb{C}$-algebra $\mathbb{C}[x, y]$, and define algebra automorphisms σ and τ of A by
$$\sigma(x) = y, \quad \sigma(y) = x$$
and
$$\tau(x) = x, \quad \tau(y) = \xi y,$$
where $\xi \in \mathbb{C}$ is a primitive third root of unity (namely, $\xi \neq 1$ and $\xi^3 = 1$). Let G be the group of algebra automorphisms of A generated by σ and τ. Define
$$A^G = \{f \in A \mid \phi(f) = f \text{ for all } \phi \in G\}.$$
Then A^G is a subalgebra of A – you do not need to prove this. Describe the algebra A^G by finding a set of generators and a set of relations.

Algebra Prelim
September 12, 2011

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Let $\mathrm{GL}_2(\mathbb{C})$ be the general linear group of 2×2 complex matrices, let H be the subgroup of $\mathrm{GL}_2(\mathbb{C})$ consisting of non-zero multiples of the identity matrix, and let $\mathrm{PGL}_2(\mathbb{C})$ be the quotient group $\mathrm{GL}_2(\mathbb{C})/\mathrm{H}$.

   Let $A, B \in \mathrm{PGL}_2(\mathbb{C})$, and assume that both elements have order n. Prove that there exist $C \in \mathrm{PGL}_2(\mathbb{C})$ and a positive integer m such that
   $$CBC^{-1} = A^m.$$

2. In this problem, as you apply Sylow's Theorem, state precisely which portions you are using.

   (a) Prove that there is no simple group of order 30.

   (b) Suppose that G is a simple group of order 60. Determine the number of p-Sylow subgroups of G for each prime p dividing 60, then prove that G is isomorphic to the alternating group A_5.

   Note: In the second part, you needn't show that A_5 is simple. You need only show that if there is a simple group of order 60, then it must be isomorphic to A_5.

3. Describe the Galois group and the intermediate fields of the cyclotomic extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$.

4. Let
   $$R = \mathbb{Z}[x]/(x^2 + x + 1).$$

   (a) Answer the following questions with suitable justification.

      i. Is R a Noetherian ring?

      ii. Is R an Artinian ring?

   (b) Prove that R is an integrally closed domain.

5. Let R be a commutative ring. Recall that an element r of R is *nilpotent* if $r^n = 0$ for some positive integer n and that the *nilradical* of R is the set $N(R)$ of nilpotent elements.

   (a) Prove that
   $$N(R) = \bigcap_{P \text{ prime}} P.$$
   (Hint: Given a non-nilpotent element r of R, you may wish to construct a prime ideal that does not contain r or its powers.)

   (b) Given a positive integer m, determine the nilradical of $\mathbb{Z}/(m)$.

   (c) Determine the nilradical of $\mathbb{C}[x, y]/(y^2 - x^3)$.

   (d) Let $p(x, y)$ be a polynomial in $\mathbb{C}[x, y]$ such that for any complex number a, $p(a, a^{3/2}) = 0$. Prove that $p(x, y)$ is divisible by $y^2 - x^3$.

6. Given a finite group G, recall that its *regular representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by left multiplication of G on itself and its *adjoint representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by conjugation of G on itself.

   (a) Let $G = \mathrm{GL}_2(\mathbb{F}_2)$. Describe the number and dimensions of the irreducible representations of G. Then describe the decomposition of its regular representation as a direct sum of irreducible representations.

   (b) Let H be a group of order 12. Show that its adjoint representation is reducible; that is, there is an H-invariant subspace of $\mathbb{C}[H]$ besides 0 and $\mathbb{C}[H]$.

7. Let M, N be finitely generated modules over $\mathbb{Z}$. Recall that $\mathrm{Ann}(M)$ is the ideal in $\mathbb{Z}$ defined as follows:
   $$\mathrm{Ann}(M) = \{a \in \mathbb{Z} \mid am = 0 \text{ for any } m \in M\}$$
   Prove that $M \otimes_{\mathbb{Z}} N = 0$ if and only if $\mathrm{Ann}(M) + \mathrm{Ann}(N) = (1)$.

8. Let R be a commutative integral domain. Show that the following are equivalent:

   (a) R is a field;

   (b) R is a semi-simple ring;

   (c) Any R-module is projective.

2010 Algebra Prelim

August 31, 2010

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count for more than several partial solutions. Always justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Let p be a positive prime number, $\mathbb{F}_p$ the field with p elements, and let $G = \mathrm{GL}_2(\mathbb{F}_p)$.
   (a) Compute the order of G, $|G|$.
   (b) Write down an explicit isomorphism from $\mathbb{Z}/p\mathbb{Z}$ to
   $$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{F}_p \right\}.$$
   (c) How many subgroups of order p does G have?
   Hint: compute gug^{-1} for $g \in G$ and $u \in U$; use this to find the size of the normalizer of U in G.

2. (a) Give definitions of the following terms: (i) a finite length (left) module, (ii) a composition series for a module, and (iii) the length of a module,
   (b) Let $l(M)$ denote the length of a module M. Prove that if
   $$0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$$
   is an exact sequence of modules of finite length, then
   $$\sum_{i=1}^{n} (-1)^i l(M_i) = 0.$$

3. Let $\mathbb{F}$ be a field of characteristic p, and G a group of order p^n. Let $R = \mathbb{F}[G]$ be the group ring (group algebra) of G over $\mathbb{F}$, and let $u := \sum_{x \in G} x$ (so u is an element of R).
   (a) Prove that u lies in the center of R.

(b) Verify that Ru is a 2-sided ideal of R.

(c) Show there exists a positive integer k such that $u^k = 0$. Conclude that for such a k, $(Ru)^k = 0$.

(d) Show that R is **not** a semi-simple ring. (**Warning:** Please use the definition of a semisimple ring; do **not** use the result that a finite length ring fails to be semisimple if and only if it has a non-zero nilpotent ideal.)

4. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ (where $a_n \neq 0$) and let $R = \mathbb{Z}[x]/(f)$. Prove that R is a finitely-generated module over $\mathbb{Z}$ if and only if $a_n = \pm 1$.

5. Consider the ring

$$S = C[0,1] = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$$

with the usual operations of addition and multiplication of functions.

(a) What are the invertible elements of S?

(b) For $a \in [0,1]$, define $I_a = \{f \in S \mid f(a) = 0\}$. Show that I_a is a maximal ideal of S.

(c) Show that the elements of any proper ideal of S have a common zero, i.e., if I is a proper ideal of S, then there exists $a \in [0,1]$ such that $f(a) = 0$ for all $f \in I$. Conclude that every maximal ideal of S is of the form I_a for some $a \in [0,1]$.
Hint: as $[0,1]$ is compact, every open cover of $[0,1]$ contains a finite subcover.

6. (a) Let L/F be a field extension that is finite and Galois. Show that if the Galois group $\mathrm{Gal}(L/F)$ is abelian then for every intermediate field $F \subseteq K \subseteq L$, K/F is also a Galois extension.

(b) Let $K = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right) \subset \mathbb{R}$. Show that $K/\mathbb{Q}$ is an extension of degree 4 that is **not** Galois.

(c) Let L be the smallest Galois extension of $\mathbb{Q}$ that contains $K = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$. Compute the group $\mathrm{Gal}(L/\mathbb{Q})$.

7. Let F be a field of characteristic zero, and let K be an **algebraic** extension of F that possesses the following property: every polynomial $f \in F[x]$ has a root in K. Show that K is algebraically closed.
Hint: if $K(\theta)/K$ is algebraic, consider $F(\theta)/F$ and its normal closure; primitive elements might be of help.

8. Let G be the unique non-abelian group of order 21.

(a) Describe all 1-dimensional complex representations of G.

(b) How many (non-isomorphic) irreducible complex representations does G have and what are their dimensions?

(c) Determine the character table of G.

Algebra Preliminary Exam **September 14, 2009**

Instructions: Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. (a) Classify groups of order $2009 = 7^2 \times 41$.

   (b) Suppose that F is a field and K/F is a Galois extension of degree 2009. How many intermediate fields are there – that is, how many fields L are there with $F \subset L \subset K$, both inclusions proper? (There may be several cases to consider.)

2. Let K be a field. A discrete valuation on K is a function $\nu : K\backslash\{0\} \to \mathbb{Z}$ such that

   (i) $\nu(ab) = \nu(a) + \nu(b)$

   (ii) ν is surjective

   (iii) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}\ \forall\ a, b \in K\backslash\{0\}$ with $a + b \neq 0$

   Let $R := \{x \in K\backslash\{0\} : \nu(x) \geq 0\} \cup \{0\}$. Then R is called the valuation ring of ν.

   Prove the following:

   (a) R is a subring of K containing the 1 in K.

   (b) for all $x \in K\backslash\{0\}$, either x or x^{-1} is in R.

   (c) x is a unit of R if and only if $\nu(x) = 0$.

   (d) Let p be a prime number, $K = \mathbb{Q}$ and $\nu_p : \mathbb{Q}\backslash\{0\} \to \mathbb{Z}$ be the function defined by $\nu_p(\frac{a}{b}) = n$ where $\frac{a}{b} = p^n \frac{c}{d}$ and p does not divide c and d. Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p.

3. Let F be a field of characteristic not equal to 2.

   (a) Prove that any extension K of F of degree 2 is of the form $F(\sqrt{D})$ where $D \in F$ is not a square in F and conversely, that each such extension has degree 2 over F.

   (b) Let $D_1, D_2 \in F$ neither of which is a square in F. Prove that $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 4$ if $D_1 D_2$ is not a square in F and is of degree 2 otherwise.

4. Let F be a field and $p(x) \in F[x]$ an irreducible polynomial.

   (a) Prove that there exists a field extension K of F in which $p(x)$ has a root.

   (b) Determine the dimension of K as a vector space over F and exhibit a vector space basis for K.

   (c) If $\theta \in K$ denotes a root of $p(x)$, express θ^{-1} in terms of the basis found in part (b).

   (d) Suppose $p(x) = x^3 + 9x + 6$. Show $p(x)$ is irreducible over $\mathbb{Q}$. If θ is a root of $p(x)$, compute the inverse of $(1 + \theta)$ in $\mathbb{Q}(\theta)$.

5. Let R be a ring and Q an R-module. According to Baer's criterion, Q is injective if and only if for every ideal I of R, any R-module map $f : I \to Q$ may be extended to an R-module map $g : R \to Q$:

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] \arrow[d, "f"'] & R \arrow[dl, dotted, "g"] \\ & Q & \end{tikzcd}$$

   (a) Suppose that p is prime and n is a positive integer with p dividing n. Then multiplication makes $\mathbb{Z}/p\mathbb{Z}$ into a module over the ring $\mathbb{Z}/n\mathbb{Z}$. Show that $\mathbb{Z}/p\mathbb{Z}$ is injective as a $\mathbb{Z}/n\mathbb{Z}$-module if and only if p^2 does not divide n.

   (b) Prove that if R is a PID, then an R-module Q is injective if and only if $rQ = Q$ for every nonzero $r \in R$.

6. Fix a ring R, an R-module M, and an R-module homomorphism $f : M \to M$.

   (a) If M satisfies the descending chain condition on submodules, show that if f is injective, then f is surjective. (Hint: note that if f is injective, so are $f \circ f$, $f \circ f \circ f$, etc.)

   (b) Give an example of a ring R, an R-module M, and an injective R-module homomorphism $f : M \to M$ which is not surjective.

   (c) If M satisfies the ascending chain condition on submodules, show that if f is surjective, then f is injective.

   (d) Give an example of a ring R, an R-module M, and a surjective R-module homomorphism $f : M \to M$ which is not injective.

7. Let G be a finite group, k an algebraically closed field, and V an irreducible k-linear representation of G.

(a) Show that $\mathrm{Hom}_{kG}(V, V)$ is a division algebra with k in its center.

(b) Show that V is finite-dimensional over k, and conclude that $\mathrm{Hom}_{kG}(V, V)$ is also finite-dimensional.

(c) Show the inclusion $k \to \mathrm{Hom}_{kG}(V, V)$ found in (a) is an isomorphism. (For $f \in \mathrm{Hom}_{kG}(V, V)$, view f as a linear transformation and consider $f - \alpha I$, where α is an eigenvalue of f.)

8. Recall the following basic definitions and facts about ideals and varieties. Let k be a field and n be a positive integer.

- If $S \subseteq k^n$, the *ideal of* S is $\mathcal{I}(S) := \{f \in k[x_1, \ldots, x_n] : f(s) = 0 \ \forall \ s \in S\}$. $\mathcal{I}(S)$ is a radical ideal in $k[x_1, \ldots, x_n]$.
- If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, then the *variety of* I in k^n is $\mathcal{V}(I) := \{s \in k^n : f(s) = 0 \ \forall \ f \in I\}$.
- If $S \subseteq k^n$, then $\mathcal{V}(\mathcal{I}(S))$ is the smallest variety containing S and is called the *Zariski closure* of S, denoted as $\overline{S}$.
- Hilbert's Nullstellensatz: If k is algebraically closed and I is an ideal in $k[x_1, \ldots, x_n]$ then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, where $\sqrt{I}$ is the radical of I.

(a) If I and J are ideals in $k[x_1, \ldots, x_n]$, the *ideal quotient* of I by J is

$$I : J = \{f \in k[x_1, \ldots, x_n] : fg \in I \ \forall \ g \in J\}.$$

You may use without proof the fact that $I : J$ is an ideal in $k[x_1, \ldots, x_n]$ containing I.

Compute $\langle xz, yz \rangle : \langle z \rangle$ in $k[x, y, z]$.

(b) Compute $\mathcal{V}(\langle xz, yz \rangle)$, $\mathcal{V}(\langle z \rangle)$ and $\mathcal{V}(\langle xz, yz \rangle : \langle z \rangle)$.

(c) Let I and J be ideals in $k[x_1, \ldots, x_n]$.

(i) Prove that $\mathcal{V}(I : J) \supseteq \overline{\mathcal{V}(I) \backslash \mathcal{V}(J)}$.

(ii) If k is algebraically closed and $I = \sqrt{I}$ then prove that $\mathcal{V}(I : J) = \overline{\mathcal{V}(I) \backslash \mathcal{V}(J)}$. (Check this statement in the example from parts (a) and (b).)

Algebra Preliminary Exam

September 8, 2008

Instructions: *Do as many problems as you can. Single complete solutions are better than several partial solutions; correct answers to four problems are sufficient to pass. Do not reprove major theorems unless asked to do so, but when you use such theorems say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.*

1. Let $f(x)$ be an irreducible polynomial of degree 5 over the field $\mathbb{Q}$ of rational numbers with exactly 3 real roots.
   (a) Show that $f(x)$ is not solvable by radicals.
   (b) Let E be the splitting field of f over $\mathbb{Q}$. Construct a Galois extension K of degree 2 over $\mathbb{Q}$ lying in E such that *no* field F strictly between K and E is Galois over $\mathbb{Q}$.

2. Let F be a finite field. Show for any positive integer n that there are irreducible polynomials of degree n in $F[x]$.

3. Show that the order of the group $GL_n(\mathbb{F}_q)$ of invertible $n \times n$ matrices over the field $\mathbb{F}_q$ of q elements is given by $(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$.

4. By looking at degrees of polynomials, show that any $\mathbb{C}$-subalgebra of the ring $\mathbb{C}[x]$ of polynomials in one variable over the complex field $\mathbb{C}$ is finitely generated.

5.(a) Let R be a commutative principal ideal domain. Show that any R-module M generated by two elements takes the form $R/(a) \oplus R/(b)$ for some $a, b \in R$. What more can you say about a and b?
   (b) Give a necessary and sufficient condition for two direct sums as in part (a) to be isomorphic as R-modules.

-over-

6. Let G be the subgroup of $GL_3(\mathbb{C})$ generated by the three matrices

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

where $i^2 = -1$. Here $\mathbb{C}$ denotes the complex field.

(a) Compute the order of G.

(b) Find a matrix in G of largest possible order (as an element of G) and compute this order.

(c) Compute the number of elements in G with this largest order.

7.(a) Let G be a group of (finite) order n. Show that any irreducible left module over the group algebra $\mathbb{C}\,G$ has complex dimension at most $\sqrt{n}$.

(b) Give an example of a group G of order $n \geq 5$ and an irreducible left module over $\mathbb{C}\,G$ of complex dimension $\lfloor\sqrt{n}\rfloor$, the greatest integer to $\sqrt{n}$.

8. Use the rational canonical form to show that any square matrix M over a field k is similar to its transpose M^t, recalling that $p(M) = 0$ for some $p \in k[t]$ if and only if $p(M^t) = 0$.

Algebra Prelim

September 18, 2007

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

The letters k and K always denote fields.

1. Let K be a field of characteristic zero and L a Galois extension of K. Let f be an irreducible polynomial in $K[x]$ of degree 7 and suppose f has no zeroes in L. Show that f is irreducible in $L[x]$.

2. Let K be a field of characteristic zero and $f \in K[x]$ an irreducible polynomial of degree n. Let L be a splitting field for f. Let G be the group of automorphisms of L which act trivially on K.

   (a) Show that G embeds in the symmetric group S_n.

   (b) For each n, give an example of a field K and polynomial f such that $G = S_n$.

   (c) What are the possible groups G when $n = 3$? Justify your answer.

3. Show there are exactly two groups of order 21 up to isomorphism.

4. (a) Show that the ring $\mathbb{Z}[i]$ of Gaussian integers is a unique factorisation domain (UFD).

   (b) Is $\mathbb{Z}[\sqrt{-5}]$ a UFD? Justify your answer.

5. Let A be a domain and K its field of fractions. Recall that we say $f \in K$ is *integral over* A if it satisfies an equation

$$f^n + a_{n-1}f^{n-1} + \cdots + a_1 f + a_0 = 0,$$

where $a_{n-1}, \ldots, a_0 \in A$. The *integral closure* $\tilde{A} \subset K$ of A is the set of $f \in K$ which are integral over A, and we say A is *integrally closed* if $\tilde{A} = A$.

   (a) Show that a UFD is integrally closed. (Hint: write f as a fraction.)

   (b) Compute the integral closure of $k[x, y]/(x^2 - y^3)$. (Remember that a polynomial ring is a UFD and therefore integrally closed.)

   (c) Compute the integral closure of $k[x, y, z]/(x^2 - y^2 z)$. (Hint: there is an obvious integral element.)

6. Let V be a finite dimensional vector space over $\mathbb{Q}$ and $A\colon V \to V$ a linear map such that $A^7 = \mathrm{id}$, the identity map. Suppose that 1 is not an eigenvalue of A. Prove that $\dim V$ is divisible by 6.

7. Let V be a vector space over a field k that is not of characteristic two. Let $\omega\colon V \times V \to k$ be a non-degenerate skew-symmetric bilinear form, i.e., $\omega(x, y) = -\omega(y, x)$ for all $x, y \in V$, and if $x \neq 0$ there is a y such that $\omega(x, y) \neq 0$.

   (a) Show that there exists a basis $e_1, \ldots, e_n, f_1, \ldots, f_n$ of V such that $\omega(e_i, e_j) = \omega(f_i, f_j) = 0$ and $\omega(e_i, f_j) = \delta_{ij}$ for all i, j. (In particular $\dim V = 2n$ is even.)

   (b) We say a subspace $W \subset V$ is *isotropic* if $\omega(w_1, w_2) = 0$ for all $w_1, w_2 \in W$. Show that the dimension of an isotropic subspace is at most $\frac{1}{2} \dim V$.

8. Let $\mathbb{H}$ be the ring of quaternions with standard basis $1, i, j, k$ and identify $\mathbb{C}$ with the subring $\mathbb{R} + \mathbb{R}i$ of $\mathbb{H}$.

   (a) Use the action of $\mathbb{H}$ on itself by left multiplication to explain why there is a ring homomorphism $\varphi : \mathbb{H} \to M_2(\mathbb{C})$, where $M_2(\mathbb{C})$ denotes the ring of 2×2 matrices. (Warning: there are two ways to view $\mathbb{H}$ as a $\mathbb{C}$-vector space, through right and left multiplication by elements in the subring $\mathbb{R} + \mathbb{R}i$.)

(b) Say why φ is injective.

(c) The special unitary group $\mathrm{SU}(2)$ consists of all 2×2 complex matrices u such that $\det(u) = 1$ and $uu^* = u^*u = 1$ where u^* is the conjugate transpose, i.e., the transpose of the matrix whose entries are the complex conjugates of the entries in u. Show that φ restricts to an isomorphism between the group of unit quaternions (those of length one) and $\mathrm{SU}(2)$.

(d) Use this to prove that $\mathrm{SU}(2)$ acts transitively on the Riemann sphere $\mathbb{CP}^1$ defined as the 1-dimensional subspaces in $\mathbb{C}^2$. (Hint: use the action of $M_2(\mathbb{C})$ on $\mathbb{C}^2$ by left multiplication.)

(e) Let $U(1)$ denote the image in $\mathrm{SU}(2)$ of the multiplicative subgroup of $\mathbb{C} - \{0\}$ consisting of the complex numbers $z \in \mathbb{C} \subset \mathbb{H}$ of length one. Show that the coset space $\mathrm{SU}(2)/U(1)$ is isomorphic to the 2-sphere S^2.

Remark. The solution to this problem gives a realization of the Hopf fibration $S^3 \to S^2$ with fibers S^1 because the group of unit quaternions is isomorphic to the 3-sphere S^3.

Algebra Preliminary Exam. **September 2006**

Instructions: *Do as many problems as you can. Single complete solutions are better than several partial solutions. Correct answers to four problems are a clear pass. Do not reprove major theorems unless asked to do so, but when you use such theorems, say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.*

1. Let $\mathbf{Z}$ be the ring of integers and let $\{0\}$ be the trivial $\mathbf{Z}$-module. Let G be a finitely generated $\mathbf{Z}$-module, i.e., a finitely generated Abelian group. Show that if $G \otimes_{\mathbf{Z}} F = \{0\}$ for all fields F, then $G = \{0\}$.

2. Let c be an automorphism of order 1 or 2 of a field F. Suppose that c has the property that for any finite set $\{a_j\}_{j \in J}$ of nonzero elements of F, $\Sigma_{j \in J} a_j c(a_j)$ is nonzero. For any $n \times n$-matrix $A = (a_{ij})$ with entries in F, let $A^c = (c(a_{ij}))$. The $n \times n$ identity matrix is denoted by I_n.

Show that if A has the property that $A(A^c)^T = I_n$, then every eigenvalue $\lambda \in F$ for A satisfies the equation $\lambda c(\lambda) = 1$.

(Remark: This result implies the familiar facts that the eigenvalues of an orthogonal matrix over the field of real numbers are in the set $\{\pm 1\}$ and that the eigenvalues of a unitary matrix over the complex numbers have absolute value 1. One takes c to be the identity map in the first case, complex conjugation in the second.)

3. (a). Let $p < q < r$ be prime integers. Show that a group of order pqr cannot be simple.

(b). Consider groups of orders $2^2 \cdot 3 \cdot p$ where p has the values 5,7 and 11. For each of those values of p, either display a simple group of order $2^2 \cdot 3 \cdot p$, or show that there cannot be a simple group of that order.

4. Let K/F be a finite Galois extension and let $n = [K : F]$. There is a theorem (often referred to as the "normal basis theorem") which states that there exists an irreducible polynomial $f(x) \in F[x]$ whose roots form a basis for K as a vector space over F. You may assume that theorem in this problem.

(a) Let $G = Gal(K/F)$. The action of G on K makes K into a finite-dimensional representation space for G over F. Prove that K is isomorphic to the regular representation for G over F.

(The regular representation is defined by letting G act on the group algebra $F[G]$ by multiplication on the left.)

(b) Suppose that the Galois group G is cyclic and that F contains a primitive n-th root of unity. Show that there exists an injective homomorphism $\chi : G \to F^\times$.

(c) Show that K contains a nonzero element a with the following property:

$$g(a) = \chi(g) \cdot a$$

for all $g \in G$.

(d) If a has the property stated in (c), show that $K = F(a)$ and that $a^n \in F^\times$.

5. Let G be the group of matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ with entries in the finite field $\mathbf{F}_p$ of p elements, where p is a prime.

(a). Prove that G is nonabelian.

(b). Suppose p is odd. Prove that $g^p = I_3$ for all $g \in G$.

(c). Suppose that $p = 2$. It is known that there are exactly two nonabelian groups of order 8, up to isomorphism: the dihedral group D_4 and the quaternionic group. Assuming this fact without proof, determine which of these groups G is isomorphic to.

6. Let $R = \mathbf{Z}[x]$, the polynomial ring in a variable x with coefficients in the integers.

(a). Let M be a maximal ideal of R. Show that R/M is a finite field.

(b). Suppose that k is any finite field. Prove that there exists at least one and no more than a finite number of maximal ideals M such that $R/M \simeq k$.

(c). Prove that no maximal ideal of R is principal, but that all nonmaximal prime ideals of R are principal.

7. There are five nonisomorphic groups of order 8. For each of those groups G, find the smallest positive integer n such that there is an injective homomorphism $\phi : G \to S_n$.

8. Let K be the field $\mathbf{Q}(z)$ of rational functions in a variable z with coeffients in the rational field $\mathbf{Q}$. Let n be a positive integer. Consider the polynomial $x^n - z \in K[x]$.

(a). Show that the polynomial $x^n - z$ is irreducible over K.

(b). Describe the splitting field of $x^n - z$ over K.

(c). Determine the Galois group of the splitting field of $x^5 - z$ over the field K.

Algebra Preliminary Exam **September 2005**

Instructions: Do as many problems as you can. Single complete solutions are better than several partial solutions. Correct answers to four problems is a pass. Do not reprove major theorems unless asked to do so, but when you use such theorems say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.

1. For any group G we define $\Omega(G)$ to be the image of the group homomorphism $\rho : G \to \mathrm{Aut}(G)$ where ρ maps $g \in G$ to the conjugation automorphism $x \to gxg^{-1}$. Starting with a group G_0, we define $G_1 = \Omega(G_0)$ and $G_{i+1} = \Omega(G_i)$ for all $i \geq 1$. If G_0 is of order p^e for a prime p and integer $e \geq 2$, prove that G_{e-1} is the trivial group.

2. Let $\mathbb{F}_2$ be the field with 2 elements.

(a) What is the order of $GL_3(\mathbb{F}_2)$?

(b) Use the fact that $GL_3(\mathbb{F}_2)$ is a simple group (which you should not prove) to find the number of elements of order 7 in $GL_3(\mathbb{F}_2)$.

3. Let G be a finite abelian group. Let $f : \mathbb{Z}^m \to G$ be a surjection of abelian groups. We may think of f as a homomorphism of $\mathbb{Z}$-modules. Let K be the kernel of f.

(a) Prove that K is isomorphic to $\mathbb{Z}^m$.

(b) We can therefore write the inclusion map $K \to \mathbb{Z}^m$ as $\mathbb{Z}^m \to \mathbb{Z}^m$ and represent it by an $m \times m$ integer matrix A. Prove that $|\det A| = |G|$.

4. Let $R = C([0,1])$ be the ring of all continuous real-valued functions on the closed interval $[0,1]$, and for each $c \in [0,1]$, denote by M_c the set of all functions $f \in R$ such that $f(c) = 0$.

(a) Prove that $g \in R$ is a unit if and only if $g(c) \neq 0$ for all $c \in [0,1]$.

(b) Prove that for each $c \in [0,1]$, M_c is a maximal ideal of R.

(c) Prove that if M is a maximal ideal of R, then $M = M_c$ for some $c \in [0,1]$. (Hint: compactness of $[0,1]$ may be relevant.)

5. Let R and S be commutative rings, and $f : R \to S$ a ring homomorphism.

(a) Show that if I is a prime ideal of S, then

$$f^{-1}(I) = \{r \in R : f(r) \in I\}$$

is a prime ideal of R.

(b) Let N be the set of nilpotent elements of R:

$$N = \{r \in R : r^m = 0 \text{ for some } m \geq 1\}.$$

N is called the *nilradical* of R. Prove that it is an ideal which is contained in every prime ideal.

(c) Part (a) lets us define a function

$$\begin{aligned} f^* : \{\text{prime ideals of } S\} &\longrightarrow \{\text{prime ideals of } R\}. \\ I &\longmapsto f^{-1}(I) \end{aligned}$$

Let N be the nilradical of R. Show that if $S = R/N$ and $f : R \to R/N$ is the quotient map, then f^* is a bijection.

6. Let F be a finite field of characteristic p. Let A be an $n \times n$ matrix over F. Suppose that A^p is the identity matrix. Show that for every polynomial $f(x)$, the characteristic polynomial of the matrix $f(A)$ is equal to $(t-c)^n$ for some c.

7. Consider the polynomial $f(x) = x^{10} + x^5 + 1 \in \mathbb{Q}[x]$ with splitting field K over $\mathbb{Q}$.

(a) Determine whether $f(x)$ is irreducible over $\mathbb{Q}$ and find $[K : \mathbb{Q}]$.

(b) Determine the structure of the Galois group $\mathbf{Gal}(K/\mathbb{Q})$.

8. For each prime number p and each positive integer n, how many elements α are there in $\mathbb{F}_{p^n}$ such that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^6}$?

Algebra Prelim
September 12, 2011

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Let $\mathrm{GL}_2(\mathbb{C})$ be the general linear group of 2×2 complex matrices, let H be the subgroup of $\mathrm{GL}_2(\mathbb{C})$ consisting of non-zero multiples of the identity matrix, and let $\mathrm{PGL}_2(\mathbb{C})$ be the quotient group $\mathrm{GL}_2(\mathbb{C})/\mathrm{H}$.

   Let $A, B \in \mathrm{PGL}_2(\mathbb{C})$, and assume that both elements have order n. Prove that there exist $C \in \mathrm{PGL}_2(\mathbb{C})$ and a positive integer m such that
   $$CBC^{-1} = A^m.$$

2. In this problem, as you apply Sylow's Theorem, state precisely which portions you are using.

   (a) Prove that there is no simple group of order 30.

   (b) Suppose that G is a simple group of order 60. Determine the number of p-Sylow subgroups of G for each prime p dividing 60, then prove that G is isomorphic to the alternating group A_5.

   Note: In the second part, you needn't show that A_5 is simple. You need only show that if there is a simple group of order 60, then it must be isomorphic to A_5.

3. Describe the Galois group and the intermediate fields of the cyclotomic extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$.

4. Let
   $$R = \mathbb{Z}[x]/(x^2 + x + 1).$$

   (a) Answer the following questions with suitable justification.

      i. Is R a Noetherian ring?

      ii. Is R an Artinian ring?

   (b) Prove that R is an integrally closed domain.

5. Let R be a commutative ring. Recall that an element r of R is *nilpotent* if $r^n = 0$ for some positive integer n and that the *nilradical* of R is the set $N(R)$ of nilpotent elements.

   (a) Prove that
   $$N(R) = \bigcap_{P \text{ prime}} P.$$
   (Hint: Given a non-nilpotent element r of R, you may wish to construct a prime ideal that does not contain r or its powers.)

   (b) Given a positive integer m, determine the nilradical of $\mathbb{Z}/(m)$.

   (c) Determine the nilradical of $\mathbb{C}[x, y]/(y^2 - x^3)$.

   (d) Let $p(x, y)$ be a polynomial in $\mathbb{C}[x, y]$ such that for any complex number a, $p(a, a^{3/2}) = 0$. Prove that $p(x, y)$ is divisible by $y^2 - x^3$.

6. Given a finite group G, recall that its *regular representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by left multiplication of G on itself and its *adjoint representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by conjugation of G on itself.

   (a) Let $G = \mathrm{GL}_2(\mathbb{F}_2)$. Describe the number and dimensions of the irreducible representations of G. Then describe the decomposition of its regular representation as a direct sum of irreducible representations.

   (b) Let H be a group of order 12. Show that its adjoint representation is reducible; that is, there is an H-invariant subspace of $\mathbb{C}[H]$ besides 0 and $\mathbb{C}[H]$.

7. Let M, N be finitely generated modules over $\mathbb{Z}$. Recall that $\mathrm{Ann}(M)$ is the ideal in $\mathbb{Z}$ defined as follows:
   $$\mathrm{Ann}(M) = \{a \in \mathbb{Z} \mid am = 0 \text{ for any } m \in M\}$$
   Prove that $M \otimes_{\mathbb{Z}} N = 0$ if and only if $\mathrm{Ann}(M) + \mathrm{Ann}(N) = (1)$.

8. Let R be a commutative integral domain. Show that the following are equivalent:

   (a) R is a field;

   (b) R is a semi-simple ring;

   (c) Any R-module is projective.

2010 Algebra Prelim

August 31, 2010

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count for more than several partial solutions. Always justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Let p be a positive prime number, $\mathbb{F}_p$ the field with p elements, and let $G = \mathrm{GL}_2(\mathbb{F}_p)$.
   (a) Compute the order of G, $|G|$.
   (b) Write down an explicit isomorphism from $\mathbb{Z}/p\mathbb{Z}$ to
   $$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{F}_p \right\}.$$
   (c) How many subgroups of order p does G have?
   Hint: compute gug^{-1} for $g \in G$ and $u \in U$; use this to find the size of the normalizer of U in G.

2. (a) Give definitions of the following terms: (i) a finite length (left) module, (ii) a composition series for a module, and (iii) the length of a module,
   (b) Let $l(M)$ denote the length of a module M. Prove that if
   $$0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$$
   is an exact sequence of modules of finite length, then
   $$\sum_{i=1}^{n} (-1)^i l(M_i) = 0.$$

3. Let $\mathbb{F}$ be a field of characteristic p, and G a group of order p^n. Let $R = \mathbb{F}[G]$ be the group ring (group algebra) of G over $\mathbb{F}$, and let $u := \sum_{x \in G} x$ (so u is an element of R).
   (a) Prove that u lies in the center of R.

(b) Verify that Ru is a 2-sided ideal of R.

(c) Show there exists a positive integer k such that $u^k = 0$. Conclude that for such a k, $(Ru)^k = 0$.

(d) Show that R is **not** a semi-simple ring. (**Warning:** Please use the definition of a semisimple ring; do **not** use the result that a finite length ring fails to be semisimple if and only if it has a non-zero nilpotent ideal.)

4. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ (where $a_n \neq 0$) and let $R = \mathbb{Z}[x]/(f)$. Prove that R is a finitely-generated module over $\mathbb{Z}$ if and only if $a_n = \pm 1$.

5. Consider the ring

$$S = C[0,1] = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$$

with the usual operations of addition and multiplication of functions.

(a) What are the invertible elements of S?

(b) For $a \in [0,1]$, define $I_a = \{f \in S \mid f(a) = 0\}$. Show that I_a is a maximal ideal of S.

(c) Show that the elements of any proper ideal of S have a common zero, i.e., if I is a proper ideal of S, then there exists $a \in [0,1]$ such that $f(a) = 0$ for all $f \in I$. Conclude that every maximal ideal of S is of the form I_a for some $a \in [0,1]$.
Hint: as $[0,1]$ is compact, every open cover of $[0,1]$ contains a finite subcover.

6. (a) Let L/F be a field extension that is finite and Galois. Show that if the Galois group $\mathrm{Gal}(L/F)$ is abelian then for every intermediate field $F \subseteq K \subseteq L$, K/F is also a Galois extension.

(b) Let $K = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right) \subset \mathbb{R}$. Show that $K/\mathbb{Q}$ is an extension of degree 4 that is **not** Galois.

(c) Let L be the smallest Galois extension of $\mathbb{Q}$ that contains $K = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$. Compute the group $\mathrm{Gal}(L/\mathbb{Q})$.

7. Let F be a field of characteristic zero, and let K be an **algebraic** extension of F that possesses the following property: every polynomial $f \in F[x]$ has a root in K. Show that K is algebraically closed.
Hint: if $K(\theta)/K$ is algebraic, consider $F(\theta)/F$ and its normal closure; primitive elements might be of help.

8. Let G be the unique non-abelian group of order 21.

(a) Describe all 1-dimensional complex representations of G.

(b) How many (non-isomorphic) irreducible complex representations does G have and what are their dimensions?

(c) Determine the character table of G.

Algebra Preliminary Exam **September 14, 2009**

Instructions: Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. (a) Classify groups of order $2009 = 7^2 \times 41$.

   (b) Suppose that F is a field and K/F is a Galois extension of degree 2009. How many intermediate fields are there – that is, how many fields L are there with $F \subset L \subset K$, both inclusions proper? (There may be several cases to consider.)

2. Let K be a field. A discrete valuation on K is a function $\nu : K\backslash\{0\} \to \mathbb{Z}$ such that

   (i) $\nu(ab) = \nu(a) + \nu(b)$

   (ii) ν is surjective

   (iii) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}\ \forall\ a, b \in K\backslash\{0\}$ with $a + b \neq 0$

   Let $R := \{x \in K\backslash\{0\} : \nu(x) \geq 0\} \cup \{0\}$. Then R is called the valuation ring of ν.

   Prove the following:

   (a) R is a subring of K containing the 1 in K.

   (b) for all $x \in K\backslash\{0\}$, either x or x^{-1} is in R.

   (c) x is a unit of R if and only if $\nu(x) = 0$.

   (d) Let p be a prime number, $K = \mathbb{Q}$ and $\nu_p : \mathbb{Q}\backslash\{0\} \to \mathbb{Z}$ be the function defined by $\nu_p(\frac{a}{b}) = n$ where $\frac{a}{b} = p^n \frac{c}{d}$ and p does not divide c and d. Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p.

3. Let F be a field of characteristic not equal to 2.

   (a) Prove that any extension K of F of degree 2 is of the form $F(\sqrt{D})$ where $D \in F$ is not a square in F and conversely, that each such extension has degree 2 over F.

   (b) Let $D_1, D_2 \in F$ neither of which is a square in F. Prove that $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 4$ if $D_1 D_2$ is not a square in F and is of degree 2 otherwise.

4. Let F be a field and $p(x) \in F[x]$ an irreducible polynomial.

   (a) Prove that there exists a field extension K of F in which $p(x)$ has a root.

   (b) Determine the dimension of K as a vector space over F and exhibit a vector space basis for K.

   (c) If $\theta \in K$ denotes a root of $p(x)$, express θ^{-1} in terms of the basis found in part (b).

   (d) Suppose $p(x) = x^3 + 9x + 6$. Show $p(x)$ is irreducible over $\mathbb{Q}$. If θ is a root of $p(x)$, compute the inverse of $(1 + \theta)$ in $\mathbb{Q}(\theta)$.

5. Let R be a ring and Q an R-module. According to Baer's criterion, Q is injective if and only if for every ideal I of R, any R-module map $f : I \to Q$ may be extended to an R-module map $g : R \to Q$:

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] \arrow[d, "f"'] & R \arrow[dl, dotted, "g"] \\ & Q & \end{tikzcd}$$

   (a) Suppose that p is prime and n is a positive integer with p dividing n. Then multiplication makes $\mathbb{Z}/p\mathbb{Z}$ into a module over the ring $\mathbb{Z}/n\mathbb{Z}$. Show that $\mathbb{Z}/p\mathbb{Z}$ is injective as a $\mathbb{Z}/n\mathbb{Z}$-module if and only if p^2 does not divide n.

   (b) Prove that if R is a PID, then an R-module Q is injective if and only if $rQ = Q$ for every nonzero $r \in R$.

6. Fix a ring R, an R-module M, and an R-module homomorphism $f : M \to M$.

   (a) If M satisfies the descending chain condition on submodules, show that if f is injective, then f is surjective. (Hint: note that if f is injective, so are $f \circ f$, $f \circ f \circ f$, etc.)

   (b) Give an example of a ring R, an R-module M, and an injective R-module homomorphism $f : M \to M$ which is not surjective.

   (c) If M satisfies the ascending chain condition on submodules, show that if f is surjective, then f is injective.

   (d) Give an example of a ring R, an R-module M, and a surjective R-module homomorphism $f : M \to M$ which is not injective.

7. Let G be a finite group, k an algebraically closed field, and V an irreducible k-linear representation of G.

(a) Show that $\mathrm{Hom}_{kG}(V, V)$ is a division algebra with k in its center.

(b) Show that V is finite-dimensional over k, and conclude that $\mathrm{Hom}_{kG}(V, V)$ is also finite-dimensional.

(c) Show the inclusion $k \to \mathrm{Hom}_{kG}(V, V)$ found in (a) is an isomorphism. (For $f \in \mathrm{Hom}_{kG}(V, V)$, view f as a linear transformation and consider $f - \alpha I$, where α is an eigenvalue of f.)

8. Recall the following basic definitions and facts about ideals and varieties. Let k be a field and n be a positive integer.

- If $S \subseteq k^n$, the *ideal of* S is $\mathcal{I}(S) := \{f \in k[x_1, \ldots, x_n] : f(s) = 0 \ \forall\ s \in S\}$. $\mathcal{I}(S)$ is a radical ideal in $k[x_1, \ldots, x_n]$.
- If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, then the *variety of* I in k^n is $\mathcal{V}(I) := \{s \in k^n : f(s) = 0 \ \forall\ f \in I\}$.
- If $S \subseteq k^n$, then $\mathcal{V}(\mathcal{I}(S))$ is the smallest variety containing S and is called the *Zariski closure* of S, denoted as $\overline{S}$.
- Hilbert's Nullstellensatz: If k is algebraically closed and I is an ideal in $k[x_1, \ldots, x_n]$ then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, where $\sqrt{I}$ is the radical of I.

(a) If I and J are ideals in $k[x_1, \ldots, x_n]$, the *ideal quotient* of I by J is

$$I : J = \{f \in k[x_1, \ldots, x_n] : fg \in I \ \forall\ g \in J\}.$$

You may use without proof the fact that $I : J$ is an ideal in $k[x_1, \ldots, x_n]$ containing I.

Compute $\langle xz, yz \rangle : \langle z \rangle$ in $k[x, y, z]$.

(b) Compute $\mathcal{V}(\langle xz, yz \rangle)$, $\mathcal{V}(\langle z \rangle)$ and $\mathcal{V}(\langle xz, yz \rangle : \langle z \rangle)$.

(c) Let I and J be ideals in $k[x_1, \ldots, x_n]$.

(i) Prove that $\mathcal{V}(I : J) \supseteq \overline{\mathcal{V}(I) \backslash \mathcal{V}(J)}$.

(ii) If k is algebraically closed and $I = \sqrt{I}$ then prove that $\mathcal{V}(I : J) = \overline{\mathcal{V}(I) \backslash \mathcal{V}(J)}$. (Check this statement in the example from parts (a) and (b).)

Algebra Preliminary Exam

September 8, 2008

Instructions: *Do as many problems as you can. Single complete solutions are better than several partial solutions; correct answers to four problems are sufficient to pass. Do not reprove major theorems unless asked to do so, but when you use such theorems say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.*

1. Let $f(x)$ be an irreducible polynomial of degree 5 over the field $\mathbb{Q}$ of rational numbers with exactly 3 real roots.
   (a) Show that $f(x)$ is not solvable by radicals.
   (b) Let E be the splitting field of f over $\mathbb{Q}$. Construct a Galois extension K of degree 2 over $\mathbb{Q}$ lying in E such that *no* field F strictly between K and E is Galois over $\mathbb{Q}$.

2. Let F be a finite field. Show for any positive integer n that there are irreducible polynomials of degree n in $F[x]$.

3. Show that the order of the group $GL_n(\mathbb{F}_q)$ of invertible $n \times n$ matrices over the field $\mathbb{F}_q$ of q elements is given by $(q^n - 1)(q^n - q) \ldots (q^n - q^{n-1})$.

4. By looking at degrees of polynomials, show that any $\mathbb{C}$-subalgebra of the ring $\mathbb{C}[x]$ of polynomials in one variable over the complex field $\mathbb{C}$ is finitely generated.

5.(a) Let R be a commutative principal ideal domain. Show that any R-module M generated by two elements takes the form $R/(a) \oplus R/(b)$ for some $a, b \in R$. What more can you say about a and b?
   (b) Give a necessary and sufficient condition for two direct sums as in part (a) to be isomorphic as R-modules.

-over-

6. Let G be the subgroup of $GL_3(\mathbb{C})$ generated by the three matrices

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

where $i^2 = -1$. Here $\mathbb{C}$ denotes the complex field.

(a) Compute the order of G.

(b) Find a matrix in G of largest possible order (as an element of G) and compute this order.

(c) Compute the number of elements in G with this largest order.

7.(a) Let G be a group of (finite) order n. Show that any irreducible left module over the group algebra $\mathbb{C}G$ has complex dimension at most $\sqrt{n}$.

(b) Give an example of a group G of order $n \geq 5$ and an irreducible left module over $\mathbb{C}G$ of complex dimension $\lfloor \sqrt{n} \rfloor$, the greatest integer to $\sqrt{n}$.

8. Use the rational canonical form to show that any square matrix M over a field k is similar to its transpose M^t, recalling that $p(M) = 0$ for some $p \in k[t]$ if and only if $p(M^t) = 0$.

Algebra Prelim

September 7, 2007

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

The letters k and K always denote fields.

1. Let K be a field of characteristic zero and L a Galois extension of K. Let f be an irreducible polynomial in $K[x]$ of degree 7 and suppose f has no zeroes in L. Show that f is irreducible in $L[x]$.

2. Let K be a field of characteristic zero and $f \in K[x]$ an irreducible polynomial of degree n. Let L be a splitting field for f. Let G be the group of automorphisms of L which act trivially on K.

   (a) Show that G embeds in the symmetric group S_n.

   (b) For each n, give an example of a field K and polynomial f such that $G = S_n$.

   (c) What are the possible groups G when $n = 3$? Justify your answer.

3. Show there are exactly two groups of order 21 up to isomorphism.

4. (a) Show that the ring $\mathbb{Z}[i]$ of Gaussian integers is a unique factorisation domain (UFD).

   (b) Is $\mathbb{Z}[\sqrt{-5}]$ a UFD? Justify your answer.

5. Let A be a domain and K its field of fractions. Recall that we say $f \in K$ is *integral over* A if it satisfies an equation

$$f^n + a_{n-1}f^{n-1} + \cdots + a_1 f + a_0 = 0,$$

where $a_{n-1}, \ldots, a_0 \in A$. The *integral closure* $\tilde{A} \subset K$ of A is the set of $f \in K$ which are integral over A, and we say A is *integrally closed* if $\tilde{A} = A$.

   (a) Show that a UFD is integrally closed. (Hint: write f as a fraction.)

   (b) Compute the integral closure of $k[x, y]/(x^2 - y^3)$. (Remember that a polynomial ring is a UFD and therefore integrally closed.)

   (c) Compute the integral closure of $k[x, y, z]/(x^2 - y^2 z)$. (Hint: there is an obvious integral element.)

6. Let V be a finite dimensional vector space over $\mathbb{Q}$ and $A\colon V \to V$ a linear map such that $A^7 = \mathrm{id}$, the identity map. Suppose that 1 is not an eigenvalue of A. Prove that $\dim V$ is divisible by 6.

7. Let V be a vector space over a field k that is not of characteristic two. Let $\omega\colon V \times V \to k$ be a non-degenerate skew-symmetric bilinear form, i.e., $\omega(x, y) = -\omega(y, x)$ for all $x, y \in V$, and if $x \neq 0$ there is a y such that $\omega(x, y) \neq 0$.

   (a) Show that there exists a basis $e_1, \ldots, e_n, f_1, \ldots, f_n$ of V such that $\omega(e_i, e_j) = \omega(f_i, f_j) = 0$ and $\omega(e_i, f_j) = \delta_{ij}$ for all i, j. (In particular $\dim V = 2n$ is even.)

   (b) We say a subspace $W \subset V$ is *isotropic* if $\omega(w_1, w_2) = 0$ for all $w_1, w_2 \in W$. Show that the dimension of an isotropic subspace is at most $\frac{1}{2} \dim V$.

8. Let $\mathbb{H}$ be the ring of quaternions with standard basis $1, i, j, k$ and identify $\mathbb{C}$ with the subring $\mathbb{R} + \mathbb{R}i$ of $\mathbb{H}$.

   (a) Use the action of $\mathbb{H}$ on itself by left multiplication to explain why there is a ring homomorphism $\varphi : \mathbb{H} \to M_2(\mathbb{C})$, where $M_2(\mathbb{C})$ denotes the ring of 2×2 matrices. (Warning: there are two ways to view $\mathbb{H}$ as a $\mathbb{C}$-vector space, through right and left multiplication by elements in the subring $\mathbb{R} + \mathbb{R}i$.)

(b) Say why φ is injective.

(c) The special unitary group SU(2) consists of all 2×2 complex matrices u such that $\det(u) = 1$ and $uu^* = u^*u = 1$ where u^* is the conjugate transpose, i.e., the transpose of the matrix whose entries are the complex conjugates of the entries in u. Show that φ restricts to an isomorphism between the group of unit quaternions (those of length one) and SU(2).

(d) Use this to prove that SU(2) acts transitively on the Riemann sphere $\mathbb{CP}^1$ defined as the 1-dimensional subspaces in $\mathbb{C}^2$. (Hint: use the action of $M_2(\mathbb{C})$ on $\mathbb{C}^2$ by left multiplication.)

(e) Let $U(1)$ denote the image in SU(2) of the multiplicative subgroup of $\mathbb{C} - \{0\}$ consisting of the complex numbers $z \in \mathbb{C} \subset \mathbb{H}$ of length one. Show that the coset space $\mathrm{SU}(2)/U(1)$ is isomorphic to the 2-sphere S^2.

Remark. The solution to this problem gives a realization of the Hopf fibration $S^3 \to S^2$ with fibers S^1 because the group of unit quaternions is isomorphic to the 3-sphere S^3.

Algebra Preliminary Exam. **September 2006**

Instructions: *Do as many problems as you can. Single complete solutions are better than several partial solutions. Correct answers to four problems are a clear pass. Do not reprove major theorems unless asked to do so, but when you use such theorems, say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.*

1. Let $\mathbf{Z}$ be the ring of integers and let $\{0\}$ be the trivial $\mathbf{Z}$-module. Let G be a finitely generated $\mathbf{Z}$-module, i.e., a finitely generated Abelian group. Show that if $G \otimes_{\mathbf{Z}} F = \{0\}$ for all fields F, then $G = \{0\}$.

2. Let c be an automorphism of order 1 or 2 of a field F. Suppose that c has the property that for any finite set $\{a_j\}_{j\in J}$ of nonzero elements of F, $\Sigma_{j\in J} a_j c(a_j)$ is nonzero. For any $n \times n$-matrix $A = (a_{ij})$ with entries in F, let $A^c = (c(a_{ij}))$. The $n \times n$ identity matrix is denoted by I_n.

Show that if A has the property that $A(A^c)^T = I_n$, then every eigenvalue $\lambda \in F$ for A satisfies the equation $\lambda c(\lambda) = 1$.

(Remark: This result implies the familiar facts that the eigenvalues of an orthogonal matrix over the field of real numbers are in the set $\{\pm 1\}$ and that the eigenvalues of a unitary matrix over the complex numbers have absolute value 1. One takes c to be the identity map in the first case, complex conjugation in the second.)

3. (a). Let $p < q < r$ be prime integers. Show that a group of order pqr cannot be simple.

(b). Consider groups of orders $2^2 \cdot 3 \cdot p$ where p has the values 5,7 and 11. For each of those values of p, either display a simple group of order $2^2 \cdot 3 \cdot p$, or show that there cannot be a simple group of that order.

4. Let K/F be a finite Galois extension and let $n = [K : F]$. There is a theorem (often referred to as the "normal basis theorem") which states that there exists an irreducible polynomial $f(x) \in F[x]$ whose roots form a basis for K as a vector space over F. You may assume that theorem in this problem.

(a) Let $G = Gal(K/F)$. The action of G on K makes K into a finite-dimensional representation space for G over F. Prove that K is isomorphic to the regular representation for G over F.

(The regular representation is defined by letting G act on the group algebra $F[G]$ by multiplication on the left.)

(b) Suppose that the Galois group G is cyclic and that F contains a primitive n-th root of unity. Show that there exists an injective homomorphism $\chi : G \to F^\times$.

(c) Show that K contains a nonzero element a with the following property:

$$g(a) = \chi(g) \cdot a$$

for all $g \in G$.

(d) If a has the property stated in (c), show that $K = F(a)$ and that $a^n \in F^\times$.

5. Let G be the group of matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ with entries in the finite field $\mathbf{F}_p$ of p elements, where p is a prime.

(a). Prove that G is nonabelian.

(b). Suppose p is odd. Prove that $g^p = I_3$ for all $g \in G$.

(c). Suppose that $p = 2$. It is known that there are exactly two nonabelian groups of order 8, up to isomorphism: the dihedral group D_4 and the quaternionic group. Assuming this fact without proof, determine which of these groups G is isomorphic to.

6. Let $R = \mathbf{Z}[x]$, the polynomial ring in a variable x with coefficients in the integers.

(a). Let M be a maximal ideal of R. Show that R/M is a finite field.

(b). Suppose that k is any finite field. Prove that there exists at least one and no more than a finite number of maximal ideals M such that $R/M \simeq k$.

(c). Prove that no maximal ideal of R is principal, but that all nonmaximal prime ideals of R are principal.

7. There are five nonisomorphic groups of order 8. For each of those groups G, find the smallest positive integer n such that there is an injective homomorphism $\phi : G \to S_n$.

8. Let K be the field $\mathbf{Q}(z)$ of rational functions in a variable z with coeffients in the rational field $\mathbf{Q}$. Let n be a positive integer. Consider the polynomial $x^n - z \in K[x]$.

(a). Show that the polynomial $x^n - z$ is irreducible over K.

(b). Describe the splitting field of $x^n - z$ over K.

(c). Determine the Galois group of the splitting field of $x^5 - z$ over the field K.

Algebra Preliminary Exam September 2005

Instructions: Do as many problems as you can. Single complete solutions are better than several partial solutions. Correct answers to four problems is a pass. Do not reprove major theorems unless asked to do so, but when you use such theorems say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.

1. For any group G we define $\Omega(G)$ to be the image of the group homomorphism $\rho : G \to \mathrm{Aut}(G)$ where ρ maps $g \in G$ to the conjugation automorphism $x \to gxg^{-1}$. Starting with a group G_0, we define $G_1 = \Omega(G_0)$ and $G_{i+1} = \Omega(G_i)$ for all $i \geq 1$. If G_0 is of order p^e for a prime p and integer $e \geq 2$, prove that G_{e-1} is the trivial group.

2. Let $\mathbb{F}_2$ be the field with 2 elements.

(a) What is the order of $GL_3(\mathbb{F}_2)$?

(b) Use the fact that $GL_3(\mathbb{F}_2)$ is a simple group (which you should not prove) to find the number of elements of order 7 in $GL_3(\mathbb{F}_2)$.

3. Let G be a finite abelian group. Let $f : \mathbb{Z}^m \to G$ be a surjection of abelian groups. We may think of f as a homomorphism of $\mathbb{Z}$-modules. Let K be the kernel of f.

(a) Prove that K is isomorphic to $\mathbb{Z}^m$.

(b) We can therefore write the inclusion map $K \to \mathbb{Z}^m$ as $\mathbb{Z}^m \to \mathbb{Z}^m$ and represent it by an $m \times m$ integer matrix A. Prove that $|\det A| = |G|$.

4. Let $R = C([0,1])$ be the ring of all continuous real-valued functions on the closed interval $[0,1]$, and for each $c \in [0,1]$, denote by M_c the set of all functions $f \in R$ such that $f(c) = 0$.

(a) Prove that $g \in R$ is a unit if and only if $g(c) \neq 0$ for all $c \in [0,1]$.

(b) Prove that for each $c \in [0,1]$, M_c is a maximal ideal of R.

(c) Prove that if M is a maximal ideal of R, then $M = M_c$ for some $c \in [0,1]$. (Hint: compactness of $[0,1]$ may be relevant.)

5. Let R and S be commutative rings, and $f : R \to S$ a ring homomorphism.

(a) Show that if I is a prime ideal of S, then

$$f^{-1}(I) = \{r \in R : f(r) \in I\}$$

is a prime ideal of R.

(b) Let N be the set of nilpotent elements of R:

$$N = \{r \in R : r^m = 0 \text{ for some } m \geq 1\}.$$

N is called the nilradical of R. Prove that it is an ideal which is contained in every prime ideal.

(c) Part (a) lets us define a function

$$\begin{aligned} f^* : \{\text{prime ideals of } S\} &\longrightarrow \{\text{prime ideals of } R\}. \\ I &\longmapsto f^{-1}(I) \end{aligned}$$

Let N be the nilradical of R. Show that if $S = R/N$ and $f : R \to R/N$ is the quotient map, then f^* is a bijection.

6. Let F be a finite field of characteristic p. Let A be an $n \times n$ matrix over F. Suppose that A^p is the identity matrix. Show that for every polynomial $f(x)$, the characteristic polynomial of the matrix $f(A)$ is equal to $(t-c)^n$ for some c.

7. Consider the polynomial $f(x) = x^{10} + x^5 + 1 \in \mathbb{Q}[x]$ with splitting field K over $\mathbb{Q}$.

(a) Determine whether $f(x)$ is irreducible over $\mathbb{Q}$ and find $[K : \mathbb{Q}]$.

(b) Determine the structure of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

8. For each prime number p and each positive integer n, how many elements α are there in $\mathbb{F}_{p^n}$ such that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^6}$?

Algebra Preliminary Exam **September 2004**

Instructions: *Do as many problems as you can. Single complete solutions are better than several partial solutions; correct answers to four problems are usually sufficient to pass. Do not reprove major theorems unless asked to do so, but when you use such theorems say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.*

1. Characterize the set of prime numbers p such that any group of order $17p$ is abelian.

2.(a) Let L be a Galois extension of a field K of degree 4. Work out all the possibilities for the number n of fields lying strictly between K and L.

(b) Using the Galois correspondence, give an example of a *non*-Galois extension L of a field K of degree 4 such that there are no fields strictly between L and K.

3.(a) Let R be a commutative ring and M an R-module. Suppose that M has a submodule N such that both N and M/N are free as R-modules. Show that M is free as an R-module and compute its rank as a function of the ranks of N and M/N.

(b) Give an example of a commutative ring R, a free R-module M, and a submodule N such that neither N nor M/N is free as an R-module.

4. Let G be a group of order 80 with a subgroup H of order 16. By looking at the action of G on left cosets of H, show that G has a nontrivial normal subgroup.

5. Let K, L be a finite fields of the same characteristic and K^*, L^* their multiplicative groups of nonzero elements. Show that there is an injective group homomorphism from K^* into L^* if and only if there is an injective field homomorphism from K into L. Give a simple condition on the orders of K and L for such homomorphisms to exist.

-over-

6. Let R be a principal ideal domain with field of fractions K. Let K^*, U be the multiplicative groups of nonzero elements of K and units in R, respectively. Show that the quotient K^*/U is a free abelian group and give a natural set of generators for it.

7.(a) Let L be a finite Galois extension of a field K whose Galois group G is cyclic of order n. Assume that K has n distinct nth roots of 1. Letting g be a generator of G, determine the characteristic polynomial of g as a K-linear map from the vector space L to itself.

(b) Find the roots of this characteristic polynomial.

(c) Show that g has n distinct eigenvalues in K, each with multiplicity one.

(d) In particular, there is $x \in L, x \neq 0$ and $\alpha \in K$, α a primitive nth root of 1, with $gx = \alpha x$. Show that $x^n \in K$ and that L is generated over K by x.

8. A *variety* is the set of common zeros in $\mathbb{C}^n$ of some collection $\mathcal{C}$ of polynomials in $\mathbb{C}[x_1, \ldots, x_n]$. Show that any variety $\mathcal{V}$ is in fact the set of common zeros of some *finite* collection of polynomials in $\mathbb{C}[x_1, \ldots, x_n]$.

Algebra Preliminary Exam **September 2003**

Instructions. Do as many problems as you can. No one is expected to solve all the problems. Complete solutions are better than partial solutions; correct answers to four problems are usually sufficient to pass. Do not reprove major theorems unless asked to, but when you use such theorems say so. Aim for clarity; even when you don't know something it is helpful if you can say that clearly so we see that you know what you do and don't know.

Notation. The letters F, k, and K, will always denote fields. We write $\mathbb{F}_q$ for the field with q elements, and $GL_n(R)$ for the group of invertible $n \times n$ matrices with entries in a commutative ring R. We write $\mathbb{Z}_n$ for the quotient $\mathbb{Z}/n\mathbb{Z}$ viewed as both an abelian group under addition and as a ring.

Terminology. Matrices of the form

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \qquad \begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & C \end{pmatrix},$$

where A, B, C are square matrices, and so on, are called block diagonal matrices.

(1) Let G be a group with $992 = 2^5 \times 31 = 32 \times 31$ elements.
  (a) Show that G has a proper normal subgroup.
  (b) Does there exist a group of order 992 that does NOT have a normal subgroup of order 31?
  HINT: The number of elements in $GL_n(\mathbb{F}_q)$ is $(q^n-1)(q^n-q)\dots(q^n-q^{n-1})$.

(2) Let R be a commutative noetherian domain.
  (a) Prove that every non-invertible element of R can be written as a product of irreducible elements.
  (b) Let K be the field of fractions (quotient field) of R. Suppose that for every element $x \in K$ either x or x^{-1} belongs to R. Show that R has a unique maximal ideal and that every ideal of R is principal. HINT: focus on $\{x \in R \mid x^{-1} \notin R\}$; if $x, y \in R$ the hypothesis implies that either x/y or y/x is in R; you can use the result of part (a) if you wish and/or Nakayama's Lemma provided you state it correctly.

(3) (a) Prove that $\mathbb{Z}[x]/(2x-1, x^7-1) \cong \mathbb{Z}/(127)$.
  (b) Prove that $\mathbb{Z}[i]/(2i-3) \cong \mathbb{F}_{13}$.

(4) Let R be a commutative domain.
  (a) Define a torsion module over R.
  (b) Define a torsion-free module over R.
  (c) State the classification theorem for finitely generated modules over a principal ideal domain. Your statement of this theorem should allow one to determine whether two such modules are isomorphic.
  (d) Let M be an $n \times n$ matrix with entries in the field k regarded as an endomorphism of $V = k^n$. Suppose that M is NOT conjugate to a block diagonal matrix. Show there is a vector $v \in V$ for which $\{M^i v \mid i \geq 0\}$ spans V.

(5) Let R be a ring with the following properties:
- up to isomorphism R has three distinct simple left modules, S_1, S_2, and S_3;
- the endomorphism rings of these modules are $\mathrm{End}_R\, S_1 \cong \mathbb{R}$, $\mathrm{End}_R\, S_2 \cong \mathbb{C}$, $\mathrm{End}_R\, S_3 \cong \mathbb{H}$, the ring of quaternions;
- every left R-module is a direct sum of simple modules.

(a) Describe explicitly the structure of the ring R.
(b) Express R as a direct sum of simple left R-modules.

(6) (a) Define what is meant by a composition series for a module.
(b) Define length of a module.
(c) State the result that ensures your definition in (b) makes sense.
(d) Let M be a module of length two over a ring R. Show that either M has a unique simple submodule or is a direct sum of two simple modules.
(e) Give examples showing that both possibilities in (d) can occur. Be certain to say what the ring is as well as what the module is.

(7) Let $p(x) = x^3 - 5 \in K[x]$ and let F be a splitting field for p over K.
(a) What are the possible Galois groups $G = \mathrm{Gal}(F/K)$? Give reasons.
(b) For each possible G describe a field K such that $G = \mathrm{Gal}(F/K)$.

(8) (a) Let G a finite group of automorphisms of a field K, and F the subfield fixed by G. Let $\{\alpha_1, \ldots, \alpha_n\}$ be the orbit of $\alpha = \alpha_1 \in K$. Show that the minimal polynomial of α over F is $g(x) := (x - \alpha_1) \ldots (x - \alpha_n)$.
(b) Let $G = \langle \sigma, \tau \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ be the group generated by the automorphisms σ and τ of the rational function field $\mathbb{C}(t)$ defined by $\sigma(t) = it^{-1}$ and $\tau(t) = -t$. Show that the fixed field of G is the rational function field $\mathbb{C}(z)$ generated by $z = t^2 - t^{-2}$.

Algebra Prelim September 16, 2002

Instructions: *Do as many problems as you can. Complete solutions are preferable to partial results. You should not reprove major theorems, but if you use a major theorem, you should state what you are using clearly. You should write enough so that there is no doubt that you know what is going on, but do not write a book when a few lines suffice.*

1. Prove that any group of order 245 must be abelian. Describe all such groups up to isomorphism.

2. (a) Let V be a simple module over the polynomial ring $R = \mathbb{R}[x]$, where $\mathbb{R}$ is the field of real numbers. Prove that V is a vector space over $\mathbb{R}$ of dimension 1 or 2.

(b) Suppose that W is a nonzero finite dimensional vector space over $\mathbb{R}$. Let A be a linear transformation of W to itself. (That is, $A \in End_{\mathbb{R}}(W)$.) Prove that there is a subspace U of W of dimension 1 or 2 such that $AU \subset U$.

3. (a) Let $G = GL_2(\mathbb{Q})$, where $\mathbb{Q}$ is the field of rational numbers. Prove that G has elements of order 2, 3, 4, and 6, but no elements of order 5.

(b) What is the smallest value of n such that $GL_n(\mathbb{Q})$ has an element of order 5.

4. Let G be a finite group of order $6m$, where $(6, m) = 1$. Suppose that g is an element of G of order 3. Prove that G has an element of order 6 if and only if the number of conjugates of g in G is odd.

5. Suppose that R is a ring. Consider an exact sequence of R-modules:

$$(*) \qquad 0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

(Recall that "exactness" means that f is injective, g is surjective, and $\ker(g) = \mathrm{im}(f)$.) We say that the exact sequence (*) splits if there is an R-module homomorphism $h : M_3 \to M_2$ such that $g \circ h : M_3 \to M_3$ is the identity map.

(a) Prove that if the exact sequence (*) splits, then M_2 is isomorphic to the direct sum $M_1 \oplus M_3$.

(b) Suppose R is the polynomial ring $\mathbb{C}[x, y]$ in two indeterminates x and y, where $\mathbb{C}$ is the field of complex numbers. Give an example of an exact sequence (*) of R-modules which does not split.

(c) Suppose that R is an integral domain and that every exact sequence (*) of R-modules splits. Prove that R is a field.

(over)

6. Let $R = \mathbb{C}[x,y]/(x^2+y^3)$, where $\mathbb{C}[x,y]$ is the polynomial ring over $\mathbb{C}$ in the indeterminates x and y. Let S be the subring $\mathbb{C}[t^2,t^3]$ of $\mathbb{C}[t]$, where $\mathbb{C}[t]$ is the polynomial ring in the indeterminate t over $\mathbb{C}$.

(a) Prove that the rings R and S are isomorphic.

(b) Let I be the ideal in R generated by the residue classes of x and y. Prove that I is a prime ideal of R, but not a principal ideal.

7. Let F be the finite field $\mathbb{Z}/5\mathbb{Z}$, where $\mathbb{Z}$ denotes the ring of integers. Let K be the splitting field over F for the polynomial $f(x) = (x^2-2)(x^3-2)(x^4-2)(x^{31}-1)$. Determine the Galois group $Gal(K/F)$.
(NOTE: It may be helpful to note that 31 divides 5^3-1.)

8. This question concerns the group ring $\mathbb{Z}[G]$ associated to a group G. By definition, $\mathbb{Z}[G]$ is the free abelian group which has the set G as a basis. That is, $\mathbb{Z}[G]$ consists of all formal finite sums $\sum_{g\in G} a_g g$, where the coefficients a_g are in $\mathbb{Z}$. One makes $\mathbb{Z}[G]$ into a ring by extending the multiplication operation on G to $\mathbb{Z}[G]$ by the distributive law. As an example, if G is an infinite cyclic group generated by x, then $\mathbb{Z}[G]$ is isomorphic to the ring $\mathbb{Z}[x,x^{-1}]$, where x is regarded as an indeterminate.

One basic property is the following: Suppose that G and H are groups. If one has a group homomorphism $f : G \to H$, then one obtains a ring homomorphism $F : \mathbb{Z}[G] \to \mathbb{Z}[H]$ defined by

$$F(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g f(g)\,.$$

You do not need to prove this basic property.

Assume that G is an abelian group. Prove that $\mathbb{Z}[G]$ is a Noetherian ring if and only if G is a finitely generated group.

Algebra Prelim
Autumn 2001

Instructions: There are eight problems altogether. Do as many problems as you can; complete solutions are preferable to partial results. You should write enough so that there is no doubt that you know what is going on, but you needn't write a lot when a few lines suffice. You should not reprove major theorems, but if you use a major result, you should clearly state what you are doing.

1. Up to isomorphism, how many groups are there of order 2001? Prove your answer. (Note: $2001 = 3 \cdot 23 \cdot 29$.)

2. Write $\mathbb{Z}^3 / \langle (1,2,3),\ (4,5,6),\ (7,8,9) \rangle$ as a product of cyclic groups. (Here, "$\langle \cdots \rangle$" denotes the subgroup generated by those elements.)

3. Suppose K is a field of characteristic $p > 0$, and let A denote the K-algebra $K[x]/(1 - x^p)$.

   (a) Define a map $\varphi : K[y] \to A$ by $\varphi(f(y)) = f(1 - x)$ for any $f(y) \in K[y]$. Show that φ is a surjective ring homomorphism, identify the kernel, and use this to get an alternate description of A.

   (b) Use part (a) to classify the finitely generated A-modules.

4. (a) Suppose R is a commutative noetherian ring. Prove that any nonzero ideal in R contains a finite product of nonzero prime ideals.

   (b) Let $R = \mathbb{C}[x, y]$. Find a nonzero ideal in R which does not contain a finite product of maximal ideals.

5. Suppose K is a field, and $f(x)$ and $g(x)$ are irreducible polynomials in $K[x]$. Let α be a root of $f(x)$ and β a root of $g(x)$.

   (a) Prove that $f(x)$ remains irreducible in $K(\beta)[x]$ if and only if $g(x)$ remains irreducible in $K(\alpha)[x]$.

   (b) Give an example where both remain irreducible.

   (c) Give an example (with $f(x)$ not proportional to $g(x)$) where neither remains irreducible.

- over -

6. Let $\zeta \in \mathbb{C}$ be a primitive 5th root of unity. Consider the polynomial $f(x) = x^5 - 3$ over the fields

   (a) $\mathbb{Q}(\zeta)$,

   (b) $\mathbb{R}$,

   (c) $\mathbb{C}$.

   For each of the cases (a)–(c), find the splitting field and the Galois group of $f(x)$. What is the order of the Galois group of $f(x)$ over the field $\mathbb{Q}$?

7. Suppose K is a field of characteristic 0, and $f(x) \in K[x]$ is an irreducible polynomial of degree 11.

   (a) Explain (with proof) why the splitting field of $f(x)$ cannot have degree 33.

   (b) Why does your proof for part (a) fail for degree 55?

8. Prove: any invertible real matrix A can be written as a product of a real symmetric positive definite matrix and an orthogonal matrix. [Hint: find a real symmetric positive definite matrix S so that $S^2 = AA^t$.]

Algebra Prelim
Autumn 2000

Instructions: Do as many problems as you can, but you needn't try to say something about every problem, especially if you don't have something to say about every problem. Complete solutions are preferable to partial results. Indeed, four complete, correct solutions constitute a passing performance. You should write enough so that there is no doubt that you know what is going on, but you needn't write a lot when a few lines suffice. You should not reprove major theorems, but if you use a major result, you should clearly state what you are using.

1. Show that every group of order 616 is solvable.

2. Let F be a field of characteristic 0 and let $f(x)$ be an irreducible polynomial of degree 4 in $F[x]$. Suppose that L is a splitting field of $f(x)$ over F.

   (a) Show that the degree $[L : F]$ is divisible by 4 and divides 24. You may quote basic facts about degrees of field extensions in towers.

   (b) Suppose α is a root of $f(x)$ in L and let $K = F[\alpha]$. Describe three qualitatively different ways that $f(x)$ might factor in $K[x]$ as a product of irreducible polynomials. For each one, describe the possible values $[L : F]$ can assume.

   (c) Give an explicit example of F, of $f(x)$, and of L for which $[L : F] = 4$. Be sure to demonstrate the irreducibility of your chosen $f(x)$ in $F[x]$.

3. Let p be a prime number and let G be a group of order $p^r m$, with r a positive integer and $(p, m) = 1$. The regular action of G on itself by left multiplication induces an action of G on the collection $\mathcal{X}$ of subsets of G of cardinality p^r. Let X be an element of $\mathcal{X}$ and let G_X be the stabilizer subgroup of X. Show that the order of G_X divides p^r.

4. Let R be a commutative ring. Recall that an element t of R is *nilpotent* if $t^n = 0$ for some positive integer n.

   (a) Suppose t is not nilpotent. Let T be the set $\{t^n : n \geq 0\}$ and let $\mathcal{I}$ be the set of ideals of R disjoint from T. Prove that $\mathcal{I}$ contains an element that is maximal with respect to inclusion; that is, show that there is an ideal M of R disjoint from T such that any ideal of R properly containing M contains an element of T.

   (b) Prove that the ideal M whose existence you have demonstrated in the first part is a prime ideal. (Hint: Suppose r and s are elements of R for which $rs \in M$. Consider the ideals $(r) + M$ and $(s) + M$.)

   (c) Let $N(R)$ be the intersection of the prime ideals of R. Prove that every element of $N(R)$ is nilpotent.

5. Let I_n denote the identity map on $\mathbb{R}^n$ and suppose that $T : \mathbb{R}^n \to \mathbb{R}^n$ is a linear map.

   (a) Suppose $n = 2$ and $T^2 = -I_2$. Prove that there are no T-eigenvectors in $\mathbb{R}^2$.

   (b) Suppose $n = 2$ and $T^2 = I_2$. Prove that $\mathbb{R}^2$ has a basis consisting of T-eigenvectors.

   (c) Suppose $n = 3$. Prove that $\mathbb{R}^3$ contains a T-eigenvector. Give an example of an operator T such that $\mathbb{R}^3$ contains a T-eigenvector, but $\mathbb{R}^3$ does not have a basis consisting of T-eigenvectors.

6. Let K be a field, let n be an integer greater than 1, and let $T : K^n \to K^n$ be a linear map. Suppose that $T^n = 0$ but $T^{n-1} \neq 0$. Prove that there is no linear map $S : K^n \to K^n$ satisfying $S^2 = T$.

7. A module M over a commutative ring R is *Artinian* if it satisfies the descending chain condition on submodules; that is, given any sequence of submodules

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$$

   of M, there is a positive integer r such that $M_r = M_{r+t}$ for any positive integer t.

   (a) Suppose K is a submodule of M such that K and M/K are Artinian. Prove that M is Artinian.

   (b) Give an example of a principal ideal domain R and an R-module M such that M is finitely generated but not Artinian.

   (c) Give an example of a principal ideal domain R and an R-module M such that M is torsion but not Artinian.

   (d) Suppose that R is a principal ideal domain and M is a finitely-generated torsion R-module. Prove that M is Artinian.

8. The four parts of this problem are independent of each other. What ties them together is that they are all "quickies"; each can be done briefly and with relative ease once you see the right path.

   (a) Let R be a commutative integral domain. Show that R can't have exactly 20 elements.

   (b) Recall that an *algebraic number* is a complex number that is algebraic over $\mathbb{Q}$. Suppose that a and $b^2 + a$ are algebraic numbers. Prove that b is an algebraic number.

   (c) Find a unique factorization domain D and two elements u and v of D such that no greatest common divisor of u and v is of the form $au + bv$ for any elements a and b of D.

   (d) Describe the prime ideals of the ring $\mathbb{Z}[x]/(x^{30}, 30)$.

Algebra Prelim
Autumn 1999

Instructions: Do as many problems as you can. Complete solutions are preferable to partial results. You should not reprove major theorems, but if you use a major theorem, you should state what you are using clearly.

1. Suppose that R is a principal ideal domain. Let M and N be finitely generated free R-modules and let $\phi : M \to N$ be an R-module homomorphism.

   (a) Let A be the kernel of ϕ, which is an R-submodule of M. Prove that A is a direct summand of M (i.e., that M contains an R-submodule B such that $M = A + B$ and $A \cap B = \{0\}$.)

   (b) Let C be the image of ϕ, which is an R-submodule of N. Show by example that C is not necessarily a direct summand of N. (Give explicit choices for R, M, N, and ϕ.)

2. Let R be a ring.

   (a) Suppose that M is a left R-module that satisfies the descending chain condition on submodules. Show that if $f : M \to M$ is an injective R-module mapping, then f is surjective. (Note that if f is injective, so is each composite $f \circ \cdots \circ f$ of f with itself n-times.)

   (b) Give an example of a ring R, an R-module M and an injective R-module homomorphism $f : M \to M$ that is not surjective.

   (c) Suppose that M is a left R-module that satisfies the ascending chain condition on submodules. Show that if $f : M \to M$ is an surjective R-module mapping, then f is injective. (Note that if f is surjective, so is each composite $f \circ \cdots \circ f$ of f with itself n-times.)

   (d) Give an example of a ring R, an R-module M and an surjective R-module homomorphism $f : M \to M$ that is not injective.

3. Let $R = \mathbb{Z}[X]$, the polynomial ring in one variable X with integral coefficients.

   (a) Prove that if k is any finite field, then there is at least one maximal ideal M of R such that R/M is isomorphic to k.

   (b) Suppose that $k = \mathbb{F}_{81}$, the field with 81 elements. Prove that R has exactly eighteen maximal ideals M such that R/M is isomorphic to k.

4. Let $R = Mat_{2\times 2}(\mathbb{C})$ be the ring of 2×2-matrices with entries in the field $\mathbb{C}$ of complex numbers, and let T be the subring of upper triangular matrices in R.

   (a) Show that the elements of a set of commuting matrices in R have an eigenvector in common.

   (b) Suppose that S is a subset of R consisting of mutually commuting matrices. Prove that there is an invertible matrix A in R such that $S \subset ATA^{-1}$.

   (c) Prove that there cannot be three commuting linearly independent matrices in R.

5. Let G be a finite group.

   (a) Show that a group of order 15 is abelian.

   (b) Show that a group of order 30 has a subgroup of order 15.

   (c) Describe all groups of order 30.

6. Suppose that G is a group. Denote the number of elements in G by $|G|$. Let $< x >$ be the cyclic subgroup of G generated by an element x. Consider the following property that a group might or might not have: If x and y are elements of G such that $< x >=< y >$, then x and y are conjugate elements of G.

   (a) Describe all abelian groups with that property.

   (b) Show that for any integer $n \geq 3$, the symmetric group S_n has that property.

   (c) Show that the alternating groups A_3 and A_4 do not have that property.

   (d) Suppose that G is a finite group with that property. Prove that if p is a prime divisor of $|G|$, then $p-1$ divides $|G|$ too.

7. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of prime degree $p \geq 3$ over the field $\mathbb{Q}$ of rational numbers. Suppose that $f(X)$ has exactly two nonreal roots. Let K be the splitting field of $f(X)$ over $\mathbb{Q}$, and let G be the Galois group of $K/\mathbb{Q}$. G can be identified with a subgroup of the symmetric group S_p, the permutation group of the roots of $f(X)$.

   (a) Show that G, as a subgroup of the symmetric group S_p, contains a transposition and a p-cycle.

   (b) Show that $G = S_p$.

8. Consider the field $F = \mathbb{Q}(t)$ of rational functions in a variable t with coefficients in the field $\mathbb{Q}$ of rational numbers. Consider the polynomial $f(X) = X^n - t \in F[X]$. Let K be the splitting field of $f(X)$ over F. Let G be the Galois group of K over F. Describe G as an abstract group for each value of $n > 1$. (Your description should be precise enough to determine G up to isomorphism as an abstract group.)

ALGEBRA PRELIM
FALL 1998

1. Let E be the splitting field over $\mathbb{Q}$ of $x^5 - 2$. Let G denote the Galois group of E over $\mathbb{Q}$.

(a) Show that $[E : \mathbb{Q}] = 20$.
(b) Show that the Sylow 5-subgroup of G is normal.
(c) Show that the Sylow 2-subgroups are not normal.
(d) What is the Galois correspondence for the Sylow 2-subgroups?

2. Let p be a prime number. Let G be the group of 3×3 upper triangular matrices over $\mathbb{Z}_p$ with 1's on the diagonal. That is,

$$G = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

(a) Show that G is a non-abelian group of order p^3.
(b) Show that if $p \neq 2$, then $x^p = 1$ for all $x \in G$.
(c) If $p = 2$ which of the non-abelian groups of order 8 is G? The dihedral or quaternion group? Explain your answer.

3.

(a) What is the automorphism group of the group of order 7?
(b) Let G be a group of order 385. Show that either G is cyclic or that its center has order 7.

4. Let D be an integer that is not a perfect square. Let $p \in \mathbb{Z}$ be a prime. Show that p is a prime in $\mathbb{Z}[\sqrt{D}]$ if and only if $x^2 - D$ is irreducible in $\mathbb{Z}_p[x]$. (Hint: consider the ideal $(p, x^2 - D)$ in $\mathbb{Z}[x]$.)

5. Let $p \in \mathbb{Z}$ be prime. Let A be the $p \times p$ matrix all of whose entries are 1. Find the Jordan normal form of A over $\mathbb{Z}_p$.

6.

(a) State the structure theorem for finitely generated modules over a P.I.D.

(b) Apply this theorem to describe the structure of the $\mathbb{Z}$-module $\mathbb{Z}^3/M$, where M is the submodule generated by $(2,-1,1)$ and $(1,1,5)$.

7. Let $i = \sqrt{-1}$. Give examples of two cyclic $\mathbb{Z}[i]$-modules, one semisimple, say M, and one not, say N. (Justify your answer.) Let I and J denote their respective annihilators. (The annihilator of a module consists of the elements x in the ring such that $xm = 0$ for every element m in the module. It is a two-sided ideal.) Determine I and J, and if possible express $\mathbb{Z}[i]/I$ and $\mathbb{Z}[i]/J$ as a direct sum of two smaller rings.

8. Let F be an infinite field. Suppose that E is a Galois extension of F with Galois group G.

(a) Show that for $a \in E$, $F(a) = E$ if and only if $\sigma(a) \neq a$ for all non-identity elements $\sigma \in G$.

(b) Show that if E is viewed as affine n-space over F, then

$$\{a \in E \mid F(a) = E\}$$

is a Zariski-open dense subset of E. (You may use the fact that the intersection of two dense open subsets of a space is dense.)

Algebra Prelim
Autumn 1997

Instructions: Do as many problems as you can, neatly. Complete solutions are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on, but do not write a book when a few lines suffice. You should not reprove major theorems (unless asked to do so), but if you use a major result, you should clearly state what you are using.

1. a. Prove that the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a Galois extension over $\mathbb{Q}$.
   b. Find the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
   c. Describe all fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

2. a. State Sylow's theorems.
   b. Up to isomorphism, how many groups of order 20 are there? Describe them.

3. Let G be a free abelian group of rank $n \geq 1$, and let G' be a subgroup of the same rank. Let $v_1, \ldots, v_n$ be a basis of G, and let $w_1, \ldots, w_n$ be a basis of G' (as $\mathbb{Z}$-modules). Write
$$w_i = \sum_{j=1}^{n} a_{ij} v_j.$$
Prove that the index $[G : G']$ is $|\det A|$, where A is the $n \times n$ matrix (a_{ij}).

4. Let $T : V \to V$ be a linear transformation, where V is an n-dimensional vector space over the field F. Say that $z \in V$ is a *cyclic vector* for T if $\{z, Tz, \ldots, T^{n-1}z\}$ is a basis for V. Prove that T has a cyclic vector if and only if the only linear transformations commuting with T are polynomials in T.

5. Let E be an extension field of $\mathbb{C}$ such that $E = \mathbb{C}(t, u)$, where t is transcendental over $\mathbb{C}$ and u satisfies $u^2 + t^2 = 1$ over $\mathbb{C}(t)$. Determine the Galois group of $\mathbb{C}(t, u)$ over $\mathbb{C}(t^n, u^n)$ for any $n \in \mathbb{N}$.

6. Recall that a commutative ring A is said to be Noetherian if it satisfies the ascending chain condition; that is, there does not exist a sequence of ideals such that
$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_j \subsetneq \cdots.$$
   a. Prove that A is Noetherian if and only if each of its ideals is finitely generated.

b. Prove that if A is Noetherian, then any A-submodule of $\underbrace{A \oplus \cdots \oplus A}_{n}$ is finitely generated, $n \in \mathbb{N}$. (Use induction on n.)

c. Again assume that A is Noetherian. Prove that any submodule of a finitely generated A-module M is finitely generated.

7. Let $A = \mathbb{R}[x, y]$. Determine all of the maximal ideals of A. For each maximal ideal $\mathfrak{m}$, find elements f and g in A such that $\mathfrak{m} = (f, g)$. (Hint: You may assume the following fact. If E is a field extension of F which is finitely generated as an F-algebra, then it is finitely generated as an F-vector space.)

8. Let $GL_n(\mathbb{C})$ denote the group of invertible $n \times n$ matrices over $\mathbb{C}$, and let

$$f : GL_n(\mathbb{C}) \to \mathbb{C}^\times$$

be a group homomorphism, where $\mathbb{C}^\times$ denotes the multiplicative group of nonzero complex numbers. Let $SL_n(\mathbb{C})$ be the subgroup of $GL_n(\mathbb{C})$ consisting of those matrices with determinant 1.

a. Prove that there exists a homomorphism $g_f : \mathbb{C}^\times \to \mathbb{C}^\times$ such that, if A is any diagonal matrix with diagonal entries $c_1, \ldots, c_n$, then

$$f(A) = g_f(c_1 c_2 \ldots c_n).$$

b. Prove that $SL_n(\mathbb{C}) \subseteq \ker f$. (Hint: Use the fact that any invertible matrix is a product of elementary matrices.)

Algebra Prelim
Autumn 1996

Instructions: Do as many problems as you can. Complete solutions are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on, but do not write a book when a few lines suffice. Be neat. You should not reprove major theorems, but if you use a major result, you should state what you are using clearly.

1. Let L be a finite Galois field extension of F with Galois group G. A field K is called an intermediate field if $F \subseteq K \subseteq L$.

   (a) Describe the one-to-one correspondence between intermediate fields K and subgroups H of G.

   (b) Suppose H_1 and H_2 are two conjugate subgroups of G. What is the relation between the corresponding intermediate fields K_1 and K_2?

   (c) Let K be an intermediate field. If K/F is a Galois extension, describe the Galois group of K/F in terms of G.

   (d) Give an example of three fields $F \subseteq K \subseteq L$ such that L is a Galois extension of F but K is not a Galois extension of F. Justify your answer.

2. Let F be the field of rational functions $\mathbb{C}(z)$ over $\mathbb{C}$ in an indeterminate z and let $f(X)$ in $F[X]$ be the polynomial $X^4 - z$.

   (a) Prove that $f(X)$ is irreducible in $F[X]$.

   (b) Describe a splitting field L for $f(X)$ over F.

   (c) Describe the Galois group of L/F.

3. In this problem, you can use the first part to answer the second and third parts.

   (a) State the classification theorem for finite abelian groups.

   (b) Suppose G is an abelian group of order 81 with a subgroup N that is cyclic of order 9 such that the quotient group G/N is also cyclic of order 9. List the possibilities for G up to isomorphism, specifying for each such G an appropriate choice of subgroup N.

   (c) Let A, B, and C be finite abelian groups such that $A \times B \cong A \times C$. Prove that $B \cong C$.

4. Let G be a finite group and let p be a prime number. Recall that if G has order $p^a t$ with t relatively prime to p, then a p-Sylow subgroup of G is a subgroup of order p^a.

   (a) Suppose G is an arbitrary group of order 60. Prove that G has exactly one or six 5-Sylow subgroups. List three possibilities for the number of 3-Sylow subgroups.

   (b) Let G be the dihedral group of order 60. Show that G has exactly one 3-Sylow subgroup and exactly one 5-Sylow subgroup. Describe a 2-Sylow subgroup of G and then state how many 2-Sylow subgroups there are.

   (c) Let G be the alternating group A_5. How many 3-Sylow subgroups does G have? How many 5-Sylow subgroups? Describe one 2-Sylow subgroup of G as an explicit set of permutations. How many 2-Sylow subgroups does G have?

5. In this problem, all rings will be assumed to be commutative with identity. Under this assumption, a ring is defined to be noetherian if it satisfies the ascending chain condition on ideals and Artinian if it satisfies the descending chain condition on ideals.

   (a) Give an example of a ring that isn't noetherian.

   (b) Must a principal ideal domain be noetherian? Prove or give a counter-example.

   (c) Give an example of a noetherian ring that isn't Artinian.

   (d) Give an example of a noetherian ring, other than a field, that is Artinian.

   (Note: One can prove in contrast that any Artinian ring is automatically noetherian.)

6. Let F be any field and let V be a finite-dimensional vector space over F. Let A and B be two linear transformations from V to itself such that $A^2 = B^2 = I_V$, where I_V denotes the identity map of V to itself. Show that if rank $(A - I_V)$ = rank $(B - I_V)$, then A and B are similar. (Hint: Consider separately the cases in which F has characteristic distinct from 2 and F has characteristic 2.)

7. Let A be an orthogonal $n \times n$ matrix; that is, A has real entries and $AA^T = I_n$.

   (a) Prove that $\det(I_n - A) \geq 0$.

   (b) Prove that $Tr(I_n - A) \geq 0$ and that equality holds if and only if $A = I_n$.

8. Recall that a group G is said to act linearly on a vector space V if there is a group action of G on V such that the action of each element of G on V is linear. A subspace W of V is called invariant with respect to the given action if $g \cdot w \in W$ for every $w \in W$ and every $g \in G$. If the only invariant subspaces of G with respect to the action are (0) and V, then the action is called irreducible.

   (a) For any prime number p, construct a finite p-group G and a linear action of G on a real vector space V of dimension greater than 1 such that the action is irreducible.

   (b) In contrast, for any prime number p, let G be a finite p-group that acts linearly on a vector space V of dimension greater than 1 over the finite field $\mathbb{F}_p$. Prove that the action isn't irreducible. (Hint: Show that in fact V contains a one-dimensional invariant subspace.)

Algebra Prelim Fall 1995

Instructions: Try to do at least five problems. In general, four *complete* solutions will constitute a pass. One complete solution will count more that two partial solutions.

1. Let F be a field and let $F^\times$ denote the group of nonzero elements of F. Show that every finite subgroup of $F^\times$ is cyclic.

2. a) State the three Sylow theorems. b) Classify up to isomorphism all groups of order 12.

3. Let S_n denote the symmetric group on n elements. Let G be a finite group.

a) Show that there is a bijective correspondence between (i) the set of conjugacy classes of homomorphisms $G \to S_n$ and (ii) the set of isomorphism classes of finite left G-sets of cardinality n. (Two group homomorphisms $f, g : H \to K$ are *conjugate* if there is an element $\sigma \in K$ such $\sigma f(x)\sigma^{-1} = g(x)$ for all $x \in H$).

b) Take $G = S_3$. Using part (a), find a "formula" for the number of conjugacy classes of homomorphisms $G \to S_n$. Your formula should express this number in terms of certain partitions of n.

4. Let L be a Galois extension of a field F, with Galois group G. Let K be an intermediate field - that is, a subfield of L containing F. Let H denote the Galois group of L over K. Show that $N_G H = H$ if and only if $Aut_F K$ is the trivial group. ($N_G H$ denotes the normalizer of H in G.)

5. a) Prove that every non-unit in a commutative Noetherian integral domain is a product of irreducible elements.

b) Let A be a Noetherian unique factorization domain, $x \in A$ a nonzero element. Show that the subring $A[x^{-1}]$ of the fraction field of A is also a Noetherian unique factorization domain.

6. Let A be a commutative algebra over $\mathbb{C}$, of dimension $n < \infty$.

a) Show that $N = \{x \in A : x^n = 0\}$ is an ideal in A (note this is the same n)

b) Show that A/N is isomorphic as an algebra to a product of d copies of $\mathbb{C}$, where d is the dimension of A/N.

7. Let V be a finite-dimensional vector space over the field $\mathbb{R}$ of real numbers, and let $T : V \to V$ be an $\mathbb{R}$-linear map. Show that T has an invariant subspace (that is, a subspace $W \subset V$ such that $TW \subset W$) of dimension one or two.

8. Let $f(x)$ be an irreducible polynomial of degree 5 over $\mathbb{Q}$ that has exactly three real roots. Show that the Galois group of the splitting field of f over $\mathbb{Q}$ is the symmetric group S_5.

Fall 1994

Algebra Prelim

1. Let G be a group.

   (a) Define the notion of a (left) group action on a set.

   (b) Write down the class equation for a group action on a finite set.

   (c) Let $Z(G)$ be the center of G. Use the class equation to prove: if G is a finite p-group, and $N \neq \{1\}$ is a normal subgroup of G, then $N \cap Z(G) \neq \{1\}$.

2. Let K be a field of characteristic 0 which contains the nth roots of 1. Let F be an extension field of K and let $a \in K$. Show that if $a^n \in K$, then $[K(a) : K]$ divides n. Give a counterexample when K does not contain the nth roots of 1.

3. Let R_o be a subring of R, both unique factorization domains. Suppose that they have the same group of units. Let a, b be nonzero elements of R_o. Let d_o (resp. d) denote their g.c.d. in R_o (resp. R).

   (a) Show that $d_o | d$ in R.

   (b) Show that d_o and d are associates in R if R_o is a PID.

   (c) Give an example where d_o and d are not associates.

4. A complex matrix A is unitary if $A\bar{A}^T = I$, i.e., if the inverse of A is its conjugate transpose. A real matrix C is orthogonal if $CC^T = I$, i.e., if it is real unitary. Show that each unitary matrix is diagonalizable by a unitary matrix. What will keep a real orthogonal matrix from being diagonalizable by a real orthogonal matrix?

5. Let G be a finite group with Sylow p-subgroups P and P' and with Sylow q-subgroups Q and Q'. Suppose that P normalizes Q and P' normalizes Q'. Show that there is an element g in G such that $gPg^{-1} = P'$ and $gQg^{-1} = Q'$.

6. Let $a_1, \ldots, a_n$ be elements of a principal ideal domain R. Show that there is an invertible $n \times n$ matrix with entries in R and with first row $(a_1, \ldots, a_n)$ if and only if $a_1, \ldots, a_n$ are relatively prime.

Hints: Recall that a free module is projective. For one direction, consider the R-module $R^n / R \cdot (a_1, \ldots, a_n)$ and use the structure theorem for PID's.

7. Let $I = (a)$ be a principal ideal in a commutative ring R with 1. Let P be a prime ideal contained in, but not equal, to I.

(a) Prove that P is contained in $\cap_{n \geq 1} I^n$.

(b) Give an example for $R = Z \oplus Z_2$ of such a $P \neq 0$ and $I \neq R$. (Z=ring of integers, Z_2 =ring of integers modulo 2.)

8. Let K be a field of characteristic other than 2 and let $K(x)$ be the field of rational functions in a variable x. Let G be the group of automorphisms of $K(x)$ generated by the automorphism determined by $x \mapsto -x$ and the automorphism determined by $x \mapsto \frac{1}{x}$. Find, as explicitly as you can, the fixed field of G.

ALGEBRA PRELIM
FALL 1993

1.

(a) State the Main Theorem of Galois Theory.

(b) Fix a prime p, let F be a subfield of C containing $\zeta = e^{2\pi i/p}$, and let $a \in F$ which is not a pth power in F. Show that the splitting field of $f(x) = x^p - a$ has degree p over F, and its Galois group is cyclic of order p.

2.

(a) State Sylow's Theorems.

(b) Prove there is no simple group of order 148.

(c) Prove there is no simple group of order 56.

3. Let G be a group of order 400 with a normal subgroup H of order 100. What is the maximum number of subgroups that G could have containing H? What is the minimum possible number of such subgroups? Prove your answer in both cases and give examples to show these bounds are attained.

4.

(a) Let F_q be the finite field of order q, and $GL_n(F_q)$ the group of $n \times n$ invertible matrices over F_q. Show that $GL_n(F_q)$ acts transitively on the d-dimensional subspaces of F_q^n if $d \leq n$; that is, if S and T are two such subspaces then there is $g \in GL_n(F_q)$ with $g \cdot S = T$.

(b) Use the result of (a) and the formula

$$|GL_n(F_q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$$

to derive a formula for the number of d-dimensional subspaces of F_q^n in terms of d and n. You will also need the formula for the number of elements in an orbit in terms of the order of the stabilizer of any element of it.

5. As in problem No.4 let F_q be the finite field of *odd* order q. If q is prime, then it is well known that F_q has a square root of -1 if and only if q is congruent to 1(mod4). Using this fact, derive a general necessary and sufficient condition on q for F_q to have a square root of -1.

6. Give an example of a Galois extension K of Q, the field of rational numbers, with non-abelian Galois group. How many intermediate fields are there between Q and K?

7. Let R be a commutative Artinian ring. Show that every prime ideal of R is maximal.

8. Let R be a commutative ring with 1. Let

$$N = \{x \in R \mid x^n = 0 \text{ for some } n\}.$$

(a) Show that N is an ideal of R contained in every prime ideal.

(b) Using Zorn's Lemma, show that N is exactly the intersection of the prime ideals of R. (Hint: suppose the result is false, and x is a non-nilpotent element contained in every prime ideal, and consider the set $S = \{1, x, x^2, \ldots\}$.)

(c) If R is noetherian, show that N is nilpotent; i.e., that $N^m = 0$ for some m.

Algebra **Fall 1992**

Preliminary Examination

There are eight problems below. Attempt as many as you can, but keep in mind that complete solutions are considerably better than partial solutions.

1. Let H be a normal subgroup of a finite group G. Fix a prime number p and let P_0 be a p-Sylow subgroup of G/H.
a.) Prove there exists a p-Sylow subgroup P of G whose image in G/H is P_0.
b.) Prove that P is unique if H is in the center of G.

2. Fix a prime number p. Let G be an abelian group, and let

$$G^* = Hom(G, \mathbb{Q}/\mathbb{Z}_{(p)}).$$

Here Hom denotes the group homomorphisms and $\mathbb{Z}_{(p)}$ is the integers localized at p under addition; that is, $\mathbb{Z}_{(p)}$ is the set of fractions a/b where p doesn't divide b. Note that G^* is an abelian group under addition of functions. Define

$$\tau : G \longrightarrow G^{**}$$

by the formula

$$(\tau(g))(f) = f(g)$$

where $f \in G^*$.
a.) Prove that τ is an isomorphism of abelian groups if G is a finite abelian p-group.
b.) Is τ an isomorphism when $G = \mathbb{Z}_{(p)}$? Justify your answer.

3. This problem asks you to recover some of the theory of finite fields. Fix a prime number p and let $\mathbb{F}_p$ be the field with p elements. Then let $\mathbb{F}_{p^n}$ be a splitting field for

$$x^{p^n} - x \in \mathbb{F}_p[x].$$

a.) Prove that $\mathbb{F}_{p^n}$ has p^n elements; in fact, prove that $\mathbb{F}_{p^n}$ consists of exactly the roots of $x^{p^n} - x$.
b.) Prove that any field with p^n elements is a splitting field for $x^{p^n} - x$ and that a finite field is uniquely determined up to isomorphism by the number of its elements.
c.) Prove that the Galois group of the extension $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ is isomorphic to $\mathbb{Z}/n$, generated by the Frobenius $\phi(a) = a^p$.
d.) Prove that $\mathbb{F}_{p^n}$ is isomorphic to a sub-field of $\mathbb{F}_{p^k}$ if and only if n divides k.

4. Let E be a finite separable extension of a field F with $[E : F] = n$. Prove that there are at most 2^n fields K with

$$F \subseteq K \subseteq E.$$

5. Recall that two $n \times n$ matrices A and B over a field are similar if there is an invertible $n \times n$ matrix Q so that

$$A = QBQ^{-1}.$$

A partition of a positive integer n is a sequence of positive integers $n_1 \geq n_2 \geq \ldots \geq n_k$ so that

$$n_1 + \cdots + n_k = n.$$

Let $P(n)$ be the number of distinct partitions of n. For example, $P(4) = 5$.
Prove that up to similarity of matrices, there are exactly $P(n)$ $n \times n$ matrices A so that $A^n = 0$ (same n).

6. Let R be a subring of a commutative ring S. Recall that an element of S is integral over R if it is a root of a polynomial with coefficients in R that has leading coefficient 1. Then S is integral over R if every element of S is integral over R.

a.) Let S be a (commutative) integral domain and $R \subseteq S$ a subring so that S is integral over R. Prove R is a field if and only if S is a field.

b.) Let $R \subseteq S$ be an inclusion of commutative rings, with S integral over R. Then prove that a prime ideal $m \subset S$ is maximal if and only if $m \cap R \subset R$ is maximal.

7. This problem asks you to recover some of the theory of semi-simple rings.

a.) Let R be a ring, not necessarily commutative. A left ideal $L \subset R$ is simple if it has no non-trivial sub-left ideals. If L_1 and L_2 are two simple left ideals, prove that either $L_1 L_2 = 0$ or there is an R-module isomorphism $L_1 \cong L_2$.

b.) Let R be a semi-simple ring; that is, $\sum L = R$ where the sum is over all simple left ideals. If $L \subseteq R$ is a simple left ideal let

$$R(L) = \sum L'$$

where this sum is over all simple left ideals L' isomorphic to L as R-modules. Prove there is a *direct* sum decomposition of left R-modules

$$\oplus R(L) = R$$

where the direct sum is over the isomorphism classes of simple left ideals.

c.) Prove that if R is semi-simple there are elements $e_1, \ldots, e_n$, each e_i in some $R(L)$, so that

$$1 = e_1 + \cdots + e_n$$

and

$$e_i^2 = e_i \qquad \text{and} \qquad e_i e_j = 0 \quad \text{if} \quad i \neq j.$$

d.) Prove that the direct sum in b.) is finite; that is, that there are only finitely many isomorphism classes of simple left ideals.

8.a.) Let A be a commutative Noetherian ring. Suppose that for every non-unit $x \in A$ there is a positive integer n so that $x^n = 0$. Prove that if $I \subset A$ is an ideal and $I \neq A$, then there is a positive integer k so that $I^k = 0$.

b.) Does this conclusion hold if A is not Noetherian? Provide a proof or a counterexample.

ALGEBRA PRELIM FALL 1991

Directions: Do as many problems as you can. Try for complete solutions.

Notation: $Z(G)$ = center of G. $N_G(A)$ = normalizer of A in G.

F_q = finite field of order q. $G(L/K)$ = Galois group of L over K.

$Tr(T)$ = trace of T. $GL_n(K)$ = the group of $n \times n$ invertible matrices with entries in K.

1. How many conjugacy classes are there in a nonabelian group of order p^3, where p is a prime? Prove your answer. (It is a polynomial in p.)

2. Suppose G is a finite group, and suppose P is a p-Sylow subgroup of G. Suppose $x, y \in Z(P)$, and suppose x and y are conjugate in G. Show that x and y are conjugate in $N_G(P)$.

3. a) Show that $GL_n(F_q)$ has order $(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})$. (HINT: How many possibilities are there for the first column of $A \in GL_n(F_q)$?)

   b) Determine the total number of 3×3 matrices over F_2 (not necessarily invertible) which are diagonalizable <u>over</u> $\underline{F_2}$.

4. Suppose M is a finitely generated module over a principal ideal domain R, and suppose that for all $x \in M$, $\text{ann}(x) = \{r \in R: rx = 0\} \neq \{0\}$. Suppose that $\phi : M \to M$ is an R-module endomorphism such that for all nonzero prime ideals P of R, the natural homomorphism $\overline{\phi} : M/PM \to M/PM$ is zero. Show that ϕ is nilpotent.

5. Suppose R is a commutative Noetherian ring with unit, and suppose that I is an ideal in R, with $I \neq R$. Show that there exists an $x \in R$ such that

$$P = \{r \in R : rx \in I\}$$

is a proper prime ideal in R.

6. Suppose V is a finite dimensional vector space over a field K, and suppose $T \in \text{Hom}_K(V,V)$ and $f(x) \in K[x]$. Show that Λ is an eigenvalue of $f(T)$ if and only if $\Lambda = f(\lambda)$ for some eigenvalue λ of T. (Λ and λ may lie in extension fields of K.)

CONTINUED OVER →

7. Let K be a field of characteristic zero. Fix an integer $n \geq 2$ and assume

(*) K contains a primitive n^{th} root of unity.

a) Let L be an extension field of K obtained by adjoining an nth root of some $a \in K$. Show that L is a Galois extension of K, with $G(L/K)$ cyclic of order dividing n.

b) Give an example showing that (a) is false without assumption (*).

8. Suppose K is a field of characteristic 0, and suppose that L is a finite Galois extension of K. If $a \in L$, denote by T_a the operation of multiplication by a (i.e. $T_a(b) = ab$), considered as a linear transformation from L, a vector space over K, to itself. That is, T_a is viewed in $\mathrm{Hom}_K(L,L)$.

a) Show that $\mathrm{Tr}(T_a) = \sum_{\sigma \in G(L/K)} \sigma(a)$.

b) Show that $\mathrm{Det}(T_a) = \prod_{\sigma \in G(L/K)} \sigma(a)$.

<u>Note</u>: The characteristic polynomial of T_a is $\prod_{\sigma \in G(L/K)} (x - \sigma(a))$.

If you use this result you must provide a proof. This may or may not be a good way to do the problem, depending on your approach. (There are several.)

Spring 1991

ALGEBRA PRELIM

Directions: Do as many problems as you can. Try for complete solutions.

1. Let $f(X) = c_n X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0$ be a polynomial with coefficients in a field. Let $A = (a_{ij})_{1 \le i,j \le n}$ be the $n \times n$-matrix whose entry a_{ij} is the coefficient of X^{2i-j} in $f(x)$. Prove that A is nilpotent if and only if $f(X)$ is a constant.

2. Find an example of a degree 12 galois field extension of $\mathbf{Q}$ which is (a) cyclic, (b) non-cyclic but abelian, (c) non-abelian. In each case give your answer in the form $\mathbf{Q}(\alpha)$ or $\mathbf{Q}(\alpha, \beta)$ for some concrete α, β. No proofs are required in this problem.

3. Let G be a finite group and H a subgroup. Recall the definitions:

$$N(H) = \{g \in G \mid gHg^{-1} = H\}; \qquad C(H) = \{g \in G \mid hg = gh \text{ for all } h \in H\}.$$

Prove that if G is a finite simple nonabelian group of even order, then either
(i) 8 divides $|G|$, or
(ii) $N(P) = C(P)$ for every 2-Sylow subgroup, or
(iii) 12 divides $|G|$.

4. This problem concerns S_n, the symmetric group on n objects.
(a) Let G be a finite cyclic p-group (p a prime), and define $K = \min\{n \mid G \hookrightarrow S_n\}$. Prove that $K = |G|$.
(b) Let G be a finite cyclic group which is **not** a p-group. Show by an example that one can have $K < |G|$.
(c) Describe the conjugacy classes in S_4.

5. Let K be a field of characteristic not 2, and let G be the group of all 2×2-matrices with entries in K and determinant 1. Let $H_1 \subset G$ be the subgroup consisting of elements of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in K$, and let $H_2 \subset G$ be the subgroup consisting of elements of the form $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$, $\alpha, \beta \in K$. Find a condition on K which is necessary and sufficient for H_1 to be isomorphic to H_2. In the case when this condition is fulfilled, construct an isomorphism between H_1 and H_2.

(CONTINUED ON NEXT PAGE)

6. Let R be a commutative ring with 1, $1 \neq 0$. Prove that there exists a polynomial $f(X) \in R[X]$ such that

$$f(r) = \begin{cases} 0, & \text{if } r = 0; \\ 1, & \text{if } r \in R \text{ is nonzero} \end{cases}$$

if and only if R is a finite field.

7. Let $\mathcal{P}(n) = \{\text{one-dimensional linear subspaces of } \mathbf{R}^n\}$, and let $SO(k) = \{k \times k$ real matrices $A \mid \|Ax\| = \|x\|$ for all $x \in \mathbf{R}^k$, and $\det A = 1\}$, $k \in \mathbf{N}^+$. Define an action of $SO(n)$ on $\mathcal{P}(n)$, prove that the action is transitive, and show that it leads to the identification: $\mathcal{P}(n) = SO(n)/SO(n-1)$ as left $SO(n)$-sets.

8. (a) Let R be a commutative ring with identity which is Noetherian. Let M be a finitely generated R-module, and let $f : M \longrightarrow M$ be an onto R-homomorphism. Prove that f is an isomorphism.

(b) Give an example showing that without the assumption that M is finitely generated, an onto R-homomorphism $f : M \longrightarrow M$ is **not** necessarily an isomorphism.

Algebra Prelim **Fall 1990**

Directions: Do as many problems as you can. One complete solution is better than two partial solutions.

1. A commutative ring R has the descending chain condition if every decreasing chain of ideals $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ has finite length.

   (a) Show that a commutative ring with the descending chain condition has only finitely many minimal prime ideals. (Actually, all its prime ideals are minimal prime ideals.)

   (b) Let $k[x]$ be the polynomial ring in one variable over a field k and let n be a positive integer. Does the ring $k[x]/(x^n)$ have the descending chain condition? Explain your answer.

   (c) What are the prime ideals of $k[x]/(x^n)$?

2. (a) Find a Galois extension field F of the rational field $\mathbb{Q}$ of degree 18.

   (b) For your extension F of $\mathbb{Q}$ in (a), what are all the intermediate fields? Which are Galois extensions of $\mathbb{Q}$?

3. (a) Find four non-isomorphic groups of order 66.

   (b) Show that the four groups in (a) are the only groups of order 66, up to isomorphism.

4. Let $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ be the space of real linear transformations from $\mathbb{R}^n$ to $\mathbb{R}$. Let $f_1, \ldots, f_m$ be elements of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$. Define a symmetric bilinear form on $\mathbb{R}^n$ by $\langle X, Y \rangle = \sum_{i=1}^{m} f_i(X) f_i(Y)$, for $X, Y \in \mathbb{R}^n$.

   f_i

   Show that the form $\langle \ , \ \rangle$ is non-degenerate if and only if $\{f_i\}_{i=1}^{m}$ spans $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$.

   (A symmetric bilinear form $\langle \ , \ \rangle$ is non-degenerate if each non-zero vector X in $\mathbb{R}^n$ may be paired with a vector Y in $\mathbb{R}^n$ so that $\langle X, Y \rangle \neq 0$.)

TURN OVER $\longrightarrow$

5. Let G be a finite group of invertible linear transformations of $\mathbb{Q}^n$. Let $\{u_1, \ldots, u_m\}$ be a set of vectors in $\mathbb{Q}^n$ which G transforms transitively. Show that $\sum_{g \in G} g \cdot u_1$ is an integer multiple of $u_1 + \cdots + u_m$.

   (G transforms $\{u_1, \ldots, u_m\}$ <u>transitively</u> if $G \cdot u_1 = \{g \cdot u_1 | g \in G\}$ equals $\{u_1, \ldots, u_m\}$.)

6. Let $k[X, Y]$ be the polynomial ring in two variables X, Y over a field k. Let $R = k[X, XY, XY^2, \ldots]$ be the subring of $k[X, Y]$ that is generated by $\{XY^j]_{j=0}^{\infty}$. Is R a Noetherian ring or not? Give a reason for your answer.

7. Let $n \geq 2$ be an integer. Let $\{e_1, \ldots, e_n\}$ be the standard basis for $\mathbb{R}^n$. The symmetry group G of the n-dimensional cube in $\mathbb{R}^n$ equals $S_n K = \{\sigma\tau | \sigma \in S_n, \tau \in K\}$ where S_n is the group of permutations of $\{e_1, \ldots, e_n\}$ and K is the group of sign changes of $\{e_1, \ldots, e_n\}$, i.e., $\sigma \in S_n$ transforms e_i to $e_{\sigma(i)}$ and $\tau \in K$ transforms each e_i to either e_i or $-e_i$.

   (a) Show which of the subgroups S_n, K is normal in G and which is not normal in G.

   (b) What is the order of K? What is the order of G? What is the structure of K? Explain your answers.

8. Let A and B be real $n \times n$ matrices.

   (a) Show that if A and B are skew-symmetric, then the commutator $[A, B] = AB - BA$ is also skew-symmetric.

   (b) Show that if A and B are symmetric, then the combination $(A, B) = AB + BA$ is also symmetric.

   (c) If A and B are symmetric, when is the commutator $[A, B] = AB - BA$ also symmetric?

ALGEBRA PRELIM SPRING 1990

Directions: Do as many problems as you can.
One complete solution is better than two partial solutions.

1. Let V be an n-dimensional vector space over a field of characteristic zero. Let $T : V \to V$ be a linear transformation. Suppose that T is idempotent (that is, $T^2 = T$).

   (a) Let $1 - T : V \to V$ be given by $(1 - T)x = x - Tx$ for $x \in V$. Prove that $1 - T$ is also idempotent.

   (b) Let W_1 = Image of T and W_2 = Image of $1 - T$. Prove that V is the direct sum of W_1 and W_2.

   (c) What are the possibilities for the minimal polynomial and the Jordan form of T?

2. Let G be a finite abelian group. For every $n \geq 1$, let $f_G(n)$ = the number of elements of G of order n. Prove that the function f_G determines G up to isomorphism.

3. (a) Let G be a finite p-group, where p is a prime. Let $\rho : G \to \mathrm{Aut}(V)$ be a homomorphism. (Here V is a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ with dimension ≥ 1. $\mathrm{Aut}(V)$ is the group of invertible linear transformations of V.) Prove that V contains a vector $v \neq 0$ such that $\rho(g)v = v$ for all $g \in G$.

   (b) Let G be a finite p-group. Let $n \geq 1$. Assume $G \subseteq GL_n(\mathbb{Z}/p\mathbb{Z})$. Let U = the group of triangular matrices with 1's on the main diagonal. Prove that $SGS^{-1} \subseteq U$ for some matrix $S \in GL_n(\mathbb{Z}/p\mathbb{Z})$.

4. Let R be a commutative ring with identity. Let I_1, I_2 be two ideals of R which are relatively prime in the sense that $I_1 + I_2 = R$. Let $I = I_1 \cap I_2$. Prove that there is a ring isomorphism $R/I \cong (R/I_1) \oplus (R/I_2)$

5. (a) Give an example of a field extension in characteristic zero, $F \subseteq K$, such that $F \neq K$ but nevertheless the group of field automorphisms of K over F is trivial.

(b) Suppose that $p(x) \in F[x]$ is an irreducible polynomial of degree > 1 and that K is the splitting field of $p(x)$ over F. Is the conclusion in (a) still possible? Prove your assertion.

(c) Is the conclusion in (b) still true if $\mathrm{char}(F) \neq 0$? Give a proof or a counterexample.

6. Let R be a commutative ring with identity. Assume that R is noetherian.

(a) Prove that every non zero ideal of R contains a finite product of non zero prime ideals of R.

(b) Is the above statement true if the word prime is replaced by maximal? Give a proof or a counterexample.

7. Let K be the splitting field over $\mathbb{Q}$ for the polynomial $p(x) = x^5 - 3$.

(a) Determine $[K:\mathbb{Q}]$.

(b) Show that $\mathrm{Gal}(K/\mathbb{Q})$ is solvable by giving explicitly a sequence of subfields

$$F_0 = \mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = K$$

so that $\mathrm{Gal}(F_{i+1}/F_i)$ is cyclic of prime order. ("Explicit" <u>means</u> give generators over $\mathbb{Q}$.)

8. There are five groups (up to isomorphism) of order 8 - three abelian groups, the dihedral group and the quaternionic group. For each group of order 8 find the smallest n so that there is an injective homomorphism $g : G \to S_n$.

ALGEBRA PRELIMINARY EXAMINATION

SEPTEMBER, 1989

Three complete and correct answers will guarantee a pass. In general, one whole solution is worth more than several partial solutions.

1. Consider the set $\mathcal{S}$ of $n \times n$ matrices over the complex numbers with minimal polynomial $(t - 1)^2$. Define an equivalence relation $\sim$ on $\mathcal{S}$ by $A \sim B$ if there is an invertible $n \times n$ matrix P such that $A = PBP^{-1}$. Give a formula for the number of equivalence classes. Give a representative of each class.

2. Define an action of S_n, the symmetric group on n letters, on $\mathbb{Q}^n$ by

$$\sigma(x_1, x_2, \ldots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}), \text{ for all } \sigma \in S_n.$$

This gives $\mathbb{Q}^n$ the structure of a $\mathbb{Q}S_n$-module. Decompose $\mathbb{Q}^n$ as a direct sum of simple $\mathbb{Q}S_n$-modules.

3. Suppose that K is an extension field of $\mathbb{Q}$ of degree d, assumed to be finite.
   (a) Show that the number of field imbeddings $\sigma : K \to \mathbb{C}$ can be written as $r_1 + 2\,r_2$, where r_1 is the number of distinct field imbeddings of K into $\mathbb{R}$, and r_2 is a positive integer.
   (b) Show that $d = r_1 + 2r_2$.
   (c) Calculate r_1 and r_2 when $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$.

4. Let K be an algebraically closed field of characteristic zero.
   (a) Show that the ring $K[x,y]/(y - x^2, y^2 - x^3)$ is finite dimensional over K. Calculate its dimension. <u>Hint</u>: View the ring as a quotient of $K[x,y]/(y - x^2)$.
   (b) Find all maximal ideals of $K[x,y]$ that contain the ideal $(y - x^2, y^2 - x^3)$.

5.Let $K = \mathbb{F}_{2^n}$ be the field of 2^n elements, $n \geq 1$. Consider the following rings:

$$R_1 = K[x]/(x^2) \qquad R_2 = \mathbb{Z}/2^{n+1}\mathbb{Z} \qquad R_3 = K[t]/(t^2 - 1)$$

$$R_4 = \left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in K\right\} \quad R_5 = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in K\right\}$$

$R_6 = KG$, where G is the group of order 2.

(a) Find all of the rings isomorphic to R_6.

(b) Is R_2 isomorphic to any of the other rings?

(c) Which of these rings is semisimple?

Give a reason to support each of your answers.

6. (a) Show that the abelian group $\mathbb{Q}/\mathbb{Z}$ is the direct sum of the groups $\mathbb{Z}[1/p]/\mathbb{Z}$, where p ranges over all prime numbers. Here $\mathbb{Z}[1/p]$ denotes the subgroup of $\mathbb{Q}$ consisting of all rational numbers of the form a/p^n, where $a \in \mathbb{Z}$.

(b) Show that every proper subgroup of $\mathbb{Z}[1/p]/\mathbb{Z}$ is finite, has order divisible by p, and that $\mathbb{Z}[1/p]/\mathbb{Z}$ has a unique subgroup of order p^n, for each positive integer n .

(c) Does every finite abelian group occur as a subgroup of $\mathbb{Q}/\mathbb{Z}$? Give a reason for your answer.

7. The integral group ring $\mathbb{Z}G$ of a group G is the set of all formal $\mathbb{Z}$-linear combinations $\Sigma n_g g$ of elements of G, where only finitely many of the integers n_g are non-zero. This is made into a ring in exactly the same way as is the group algebra KG of G over a field K; thus $\mathbb{Z}G$ is a subring of $\mathbb{Q}G$. Define a function $\phi : \mathbb{Z}G \to \mathbb{Z}$ by $\phi(\Sigma n_g g) = \Sigma n_g$.

(a) Show that ϕ is a ring homomorphism.

(b) Denote the kernel of ϕ by J. Show that J is a free $\mathbb{Z}$-module with basis $\{g - 1 : g \in G, g \neq 1\}$.

(c) Denote the square of the ideal J by J^2. Consider J/J^2 as an abelian group via the addition of $\mathbb{Z}G$. Define a function $\Psi : G \to J/J^2$ by $\Psi(g) = (g - 1) + J^2$. Show that Ψ is a group homomorphism.

(d) Show that Ψ induces an isomorphism $\Psi^{ab} : G/[G,G] \to J/J^2$, where $[G,G]$ denotes the commutator subgroup of G. <u>Hint</u>: Construct a homomorphism from J to $G/[G,G]$ using (b).

8. Show that there exists an irreducible polynomial $f(x)$ in $\mathbb{Q}[x]$ of degree 14 whose splitting field is of degree 14 over $\mathbb{Q}$. <u>Hint</u>: Begin by constructing a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}/28\mathbb{Z}$.

ALGEBRA PRELIM

SPRING 1989

Directions: Do as many problems as you can. One complete solution is better than two partial solutions.

1. Let G be a group and X a finite set. Assume there is a group action of G on X. Let V be the vector space over $\mathbb{C}$ with X as basis and let each g in G act as a linear operator on V by acting on the basis X in the given way. Define Tr(g), the trace of g, to be the usual trace of g as a linear operator on V. Let $X_g = \{x \in X : g.x = x\}$.

   (i) Show that $Tr(g) = \#X_g$.

   (ii) Show for g and h in G that $\#X_{gh} = \#X_{hg}$.

   (iii) Show that $Tr(g^2) \geq Tr(g)$. Is this true in general for the trace of a linear operator?

2. Let X be the closed interval [0,1] and let $R = \{f:X \to \mathbb{R} : f \text{ is continuous}\}$. Make R into a commutative ring by pointwise addition and multiplication. For a subset Y of X, let $I_Y = \{f \in R : f(y) = 0 \text{ for all } y \in Y.\}$.

   (i) Show that I_Y is a maximal ideal of R if and only if $Y = \{y\}$ for a point y of X.

   (ii) Show that R is not a noetherian ring.

3. Let $F = \mathbb{Q}(i)$ and let f(x) be an irreducible polynomial in F[x] of degree 4. Let K be a splitting field of f(x) over F.

   (i) Give an example of f(x) for which [K:F] = 4.

   (ii) Suppose the Galois group of K/F is the alternating group A_4. How many distinct fields L are there with $F \subseteq L \subseteq K$ such that [L:F] = 3? = 4? How many of these are normal extensions of F?

Continued on page 2

4. Let A be the ring of 3x3 matrices with arbitrary entries from $\mathbb{R}$ in the indicated locations and 0 elsewhere:

$$\begin{pmatrix} * & 0 & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$$

Let V be the 3-dimensional space of column vectors on which elements of A acts on the left in the usual way. (This makes V into a left A-module.)

(i) Find two linearly independent vectors in V which are eigenvectors for A. (An eigenvector for A is a vector v such that $a.v \in \mathbb{R}.v$ for all $a \in A$.)

(ii) Using these vectors, find A-submodules $V_1 \subseteq V_2$ of V such that V_1, V_2/V_1, and V/V_2 are all simple A-modules. (An A-submodule is a subspace which is A-invariant. A simple module is one whose only submodules are 0 and itself.)

(iii) Show that no two of the three simple modules of (ii) are isomorphic A-modules.

5. Let $<\,,\,>$ be the standard inner product on $\mathbb{R}^n$. Given an nxn matrix M, let ${}^tM$ be its transpose.

(i) Show that $<Mv, w> = <v, {}^tMw>$ for any vectors v and w in $\mathbb{R}^n$.

(ii) Show that $<Mv, w> + <v, Mw> = 0$ for all v and w in $\mathbb{R}^n$ if and only if $M + {}^tM = 0$.

(iii) Suppose that M and N are matrices satisfying the condition of (ii). Must MN satisfy this condition? What about MN - NM?

6. Let G be a finite group of order 108.

(i) Why must G have a subgroup H of order 27?

(ii) Using the existence of H, find a set of four elements on which G acts and conclude that there is a non-trivial homomorphism from G into the group S_4 of permutations of a four element set.

(iii) Show that either H is a normal subgroup of G or G has a normal subgroup of order 9.

END

Math Lib. cop. 2

ALGEBRA PRELIM

Fall 1988

Directions: Do as many problems as you can. One complete solution is better than two partial solutions.

1. Prove that any group of order 45 is abelian.

2. Let $\mathbb{F}$ and $\mathbb{F}'$ be finite fields. State and prove a necessary and sufficient condition that $\mathbb{F}'$ be a subfield of $\mathbb{F}$.

3. Consider

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$$

as an element of the space of 2x2 matrices over the field of complex numbers. If n is a positive integer, then compute A^n. Hint: think eigenvalues.

4. Let $\mathbb{F}_p$ be the field of p elements where p is a prime number (i.e. $\mathbb{F}_p = \mathbb{Z}/(p)$.) The *general linear group* $Gl_n(\mathbb{F}_p)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_p$.

(a) Show that $Gl_3(\mathbb{F}_p)$ has $(p^3-1)(p^3-p)(p^3-p^2)$ elements.

(b) Show that a group H is a p-Sylow subgroup of $Gl_3(\mathbb{F}_p)$ iff with respect to a suitable basis it is precisely all elements of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, where a, b and c are elements of $\mathbb{F}_p$.

5. Let L be an extension field of degree n of a field K of characteristic 0. Using Galois theory, find a finite upper bound B(n) for the number of intermediate fields T, $K < T < L$. Here B(n) is to depend only on n, but you should not try to give a relatively small B(n). Do not assume that the extension L/K is Galois.

6. If G is a finite group, a "chief series" for G is a maximal normal series--i.e. a series of subgroups

$$G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{1\}$$

all normal in G which has no nontrivial normal refinement. (That is, there is no subgroup N with $G_i > N > G_{i+1}$ such that N is normal in G.) If G is solvable show that the factors G_i/G_{i+1} of a chief series are "elementary abelian"--that is, vector spaces over $\mathbb{Z}/(p)$ for some primes p.

7. Let V be a finite dimensional vector space over a field k and let β be a bilinear form on V such that

(i) $\beta(x,y) = \beta(y,x)$ for all x and y,

(ii) $\beta(x,x) \neq 0$ unless $x = 0$.

Show that V has a basis with respect to which the matrix of β is diagonal.

8. Give an example, with a complete justification, of each of the following:

(i) A commutative Noetherian domain which is not a principal ideal domain.

(ii) A commutative ring which is not Noetherian.

(iii) A commutative domain in which not every nonzero prime ideal is maximal.

ALGEBRA PRELIM

Spring 1988

Directions: Do as many problems as you can.
One complete solution is better than two partial solutions.

1. Let K be a field and let $G = GL_2(K)$ be the group of invertible 2×2 matrices over K.

   Let $G_1 = \{g \in G \mid \det(g) = 1\}$, and $G_2 = \{g \in G \mid g$ has lower left entry zero$\}$.

   In the diagram

$$\begin{tikzcd} & G \arrow[dl, dash] \arrow[dr, dash] & \\ G_1 \arrow[dr, dash] & & G_2 \arrow[dl, dash] \\ & G_1 \cap G_2 & \end{tikzcd}$$

   each of the four lines represents a subgroup included in a larger group.

   What are normal inclusions? Prove your answer.

2. Is it true that whenever R is a unique factorization domain (U.F.D.) and a is an irreducible element of R, then R/aR is also a U.F.D.? Explain.

3. Let A_5 be the alternating groups on five letters. Let H be a 5-Sylow subgroup of the simple group A_5.

   (a) How many elements does the normalizer of H in A_5 have?

   Let D_5 be the dihedral group of symmetries of the regular pentagon.

   (b) Construct a 1-1 homomorphism $D_5 \to A_5$.

   (c) How are your answers to (a) and (b) related?

4. Let $R = \mathbb{C}[X_1, X_2, \ldots, X_n]$ be the complex polynomial ring in n-variables.

   Let M be a finitely generated unitary R-module. Let $\varphi : R \to \mathbb{C}$ be a homomorphism of $\mathbb{C}$ - algebras.

   For each $j \geq 1$, let $M_j = \{m \in M \mid (a - \varphi(a)1)^j . m = 0$ for all $a \in R\}$

   ($\varphi(a)1$ is a constant polynomial in R).

   Must there be an index k such that $M_j = M_k$ for all $j \geq k$? Explain.

5. For each of the fields $K = \mathbb{Q}$ (rational numbers) and $K = \mathbb{C}(X)$ (the extension of the complex numbers by an indeterminate X), give an example of an extension field L such that L/K is a galois extension whose galois group is the non-cyclic group of order 4. In each example, describe a primitive element α of the extension (i.e. an element so that $L = K(\alpha)$) and give its minimal polynomial. No proofs are required in this problem.

6. Let G be the group of unitary complex $n \times n$ matrices. Consider the set of conjugacy classes of G. In each conjugacy class there is an element in Jordan canonical form. Which Jordan form matrices arise in that way? Explain.

7. Let $G = \{\pm 1, \pm 1\cdot i, \pm 1\cdot j, \pm 1\cdot k\}$ be the eight element group of units of the ring of integral quaternions. The group G may be described by the following: 1 is the identity element, $\{1, -1\}$ is the center, $i^2 = j^2 = k^2 = -1$, and $i\cdot j = k$, while $j\cdot i = -1\cdot k$.
(It follows that $i\cdot k = (-1)\cdot j$, $k\cdot i = j$, $j\cdot k = i$, $k\cdot j = -1\cdot i$)

(a) Identify the group of inner automorphisms of G.

(b) Find an outer automorphism of G of order 3.

End

ALGEBRA PRELIM

Fall 1987

Directions: Do as many of the problems as you can.
Try for complete solutions.
One complete solution is better than two partial solutions.

$\mathbb{Z}$ = ring of integers

$\mathbb{Q}$ = field of rational numbers

$\mathbb{F}_p$ = field with p elements

1. Let G be a finite group of order $p\,q\,r$, where p,q,r are distinct primes. Show that G is not a simple group.

2. Let G be a finitely generated group. Prove that for any $n \geq 1$, G can have only finitely many subgroups of index n.

3. a) Prove the existence of an irreducible polynomial over $\mathbb{Q}$ of degree 14 whose splitting field over $\mathbb{Q}$ also has degree 14.

   b) Prove the existence of an irreducible polynomial over $\mathbb{Q}$ of degree 10 whose splitting field over $\mathbb{Q}$ has degree 20.

4. Let R be a commutative ring with identity.

   a) Show that if $R[X]$ is a noetherian ring, then R must also be noetherian.

   b) Show that if $R[X]$ is a P.I.D., then R must be a field.

5. Prove that $I = (5, X^2 + 2)$ is a prime ideal in $\mathbb{Z}[X,Y]$ and that $\mathbb{Z}[X,Y]/I$ is a P.I.D.

6. Let M be a free abelian group of finite rank, and let A be an endomorphism of M. Show that M/AM is finite if and only if $\det A$ is nonzero. Show also that if $\det A \neq 0$, then M/AM has order $|\det A|$.

7. Let R be a finite dimensional algebra with identity over a field F. Prove that there are only finitely many nonisomorphic simple R-modules. Also show that there is at least one simple R-module.

8. Let G be a finite p-group, p a prime, and let A be the group ring of G over $\mathbb{F}_p$ (thus A consists of formal linear combinations $\sum_{g \in G} c_g \cdot g$, with $c_g \in \mathbb{F}_p$; the multiplication in A comes from the multiplication in G).

(a) the <u>trivial</u> A-module is $\mathbb{F}_p$ itself with the A-module structure defined by $g \cdot x = x \quad \forall g \in G, \ x \in \mathbb{F}_p$. Show that the trivial module is the only simple A-module, up to isomorphism.

(Hint: A simple A-module is in particular a finite G-set).

(b) Let $I = \{\Sigma c_g g \in A : \Sigma c_g = 0\}$. Use (a) to show that I is a nilpotent two-sided ideal.

ALGEBRA PRELIM

Spring 1987

Directions: Do as many of the problems as you can. Try for complete solutions. (One complete solution is better than two partial solutions.)

$\mathbb{Z}$ = ring of integers

$\mathbb{Q}$ = field of rational numbers

$\mathbb{C}$ = field of complex numbers

$\mathbb{F}_p$ = field with p elements

1. Show that A_5 (alternating group) has no subgroup of order 15. (You may use the fact that A_5 is a simple group.) Hence show that S_5 (symmetric group) has no subgroup of order 15.

2. Let p be a prime number. Let G be a finite group and suppose that the quotient of G by its center is a p-group. Show that G has only one p-Sylow subgroup.

3. Let (a,b), (c,d) be two elements of the free abelian group $\mathbb{Z}^2$ of rank 2. Show that these two elements generate $\mathbb{Z}^2$ if and only if $ad - bc = \pm 1$.

4. Let p be a prime number different from 2,3.
Let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$. Let ζ be a primitive cube root of 1 in $\overline{\mathbb{F}}_p$. Let $\alpha = \zeta - \zeta^{-1} \in \overline{\mathbb{F}}_p$.

   (a) Show that $\alpha \in \mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$.
   You may use standard facts about the Galois theory of finite fields.

   (b) Show that $\alpha^2 = -3$. (Hint: First show that $1 + \zeta + \zeta^2 = 0$.)

   Putting (a) and (b) together, we find that -3 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$.

5. Let n,k be two positive integers. We will say that two $\mathbb{C}$-algebra homomorphisms f_1, f_2 from $M_n(\mathbb{C})$ ($n \times n$ complex matrices) to $M_k(\mathbb{C})$ are equivalent if there exists an invertible matrix A in $M_k(\mathbb{C})$ such that $f_1(x) = Af_2(x)A^{-1}$ for all $x \in M_n(\mathbb{C})$. How many equivalence classes of such homomorphisms are there?
(Hint: Use such a homomorphism to view $\mathbb{C}^k$ as a module over $M_n(\mathbb{C})$.)

(a) Let R be the following subring of $M_2(\mathbb{C})$:

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \;\middle|\; a \in \mathbb{Q},\ b,d \in \mathbb{C} \right\}.$$

Show that R is right artinian but not left artinian. (Recall: R is right artinian if there is no infinite descending chain of right ideals.)
(<u>Hint</u>: Look at the nilpotent radical as a left R-module.)

(b) Give an example of a commutative ring which is not noetherian. Prove that your example is not noetherian.

7. (a) The numbers 20604, 20927, 53227, 78421, 25755 are all divisible by 17.

Using elementary <u>column</u> operations, prove that 17 divides the determinant of the 5×5 matrix

$$\begin{pmatrix} 2 & 0 & 6 & 0 & 4 \\ 2 & 0 & 9 & 2 & 7 \\ 5 & 3 & 2 & 2 & 7 \\ 7 & 8 & 4 & 2 & 1 \\ 2 & 5 & 7 & 5 & 5 \end{pmatrix}.$$

(b) Let $S : U \to V$, $T : V \to W$ be linear maps of complex vector spaces.

Put $n = \dim U$, $m = \dim V$.

Write $\nu(T) = \text{nullity}\,(T) = \dim\,(\ker T)$,
$\nu(S) = \text{nullity}\,(S)$,
$\nu(TS) = \text{nullity}\,(TS)$.

Prove Sylvester's law of nullity:

$\max\,\{n - m + \nu(T)\,,\ \nu(S)\} \le \nu(TS) \le \min\,\{n,\ \nu(S) + \nu(T)\}$.

---

8. Let K/F be a finite Galois extension of fields and suppose that the Galois group of K/F is isomorphic to the symmetric group S_4. How many intermediate fields L $(K \supset L \supset F)$ are there such that $[L : F] = 8$?

Show that any two such fields L are isomorphic over F.

ALGEBRA PRELIM
FALL 1986

Directions: Do as many of the problems as you can. Complete solutions are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on, but do not write a book when a few lines suffices. Be neat. You should not reprove major theorems, but if you may use a major result (e.g. the Sylow theorems or Hilbert's basis theorem), you should state what you are using clearly. In this exam, all rings have identity.

1. Let G be a group with a normal subgroup H of finite index p, for p a prime number. For an element x of H, let $C_G(x)$ be the conjugacy class of x in G and let $C_H(x)$ be the conjugacy class of x in H.

   (i) Show for $g \in G$ and $x \in H$ that $g^{-1}C_H(x)\,g$ is again a conjugacy class of H and conclude that G acts on the set of conjugacy classes of H.

   (ii) Show for $x \in H$ that $C_G(x)$ lies in H.

   (iii) Show for $x \in H$ that either $C_G(x) = C_H(x)$ or $C_G(x)$ is the disjoint union of p-many conjugacy classes of H.

2. Let R be the ring $\mathbb{Z}[x]$.

   (i) Show that there is no ring homomorphism of R **onto** the field $\mathbb{Q}$, or **onto** any field extension of $\mathbb{Q}$.

   (ii) Show that any maximal ideal of R contains a non-zero element of $\mathbb{Z}$.

   (iii) Using (ii), describe all fields K for which there is a ring homomorphism of R **onto** K.

3. Let K be the subfield of $\mathbb{C}$ obtained from $\mathbb{Q}[i]$ by adjoining $\sqrt[4]{7}$, the positive real fourth root of 7. Call this number α.

   (i) Show that K is a Galois extension of $\mathbb{Q}$, and calculate its dimension over $\mathbb{Q}$.

   (ii) Determine explicitly the Galois group of K over $\mathbb{Q}$; that is, describe what group it is and how its elements act on K or on generators of K over $\mathbb{Q}$.

4. Let A be the subring of $M_2(\mathbb{C})$ consisting of all matrices $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \; a, b, c \in \mathbb{C} \right\}$. Let V be the left A-module of column vectors $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \middle| \; x, y \in \mathbb{C} \right\}$, with elements of A acting by the usual operation, on the left, of matrices on column vectors.

(i) Show that V has a unique submodule W with $0 \neq W \neq V$, and that W is simple.

(ii) Show that V/W is also a simple A-module.

(iii) Are V and W isomorphic as A-modules?

5. Let L be an 84-dimensional field extension of a field F, with L **Galois** over F.

(i) Which of the following is true and why?

(a) There is an intermediate field extension K of dimension 21 over F.
(b) There is no intermediate field extension K of dimension 21 over F.
(c) The existence of such a K depends on the choice of L and F.

(ii) Which of the following is true and why?

(a) There is an intermediate field extension K of dimension 12 over F which is **Galois.**
(b) There is no intermediate field extension K of dimension 12 over F which is **Galois.**
(c) The existence of such a K depends on the choice of L and F.

6. The group of invertible 5x5 complex matrices acts on $M_5(\mathbb{C})$ by conjugation, and the orbits are called similarity classes (or conjugacy classes).

(i) Show that all matrices in a similarity class have the same eigenvalues.

(ii) Given a similarity class of matrices, all of which have exactly 4 distinct eigenvalues, is there a diagonal matrix in this similarity class? (yes? no? depends on the class? Justify your answer.)

(iii) How many similarity classes are there of matrices having only the single eigenvalue 2? (Explain how you get your number.)

(iv) How many of the classes in part (iii) have the property that for every matrix in the class there is a basis of $\mathbb{C}^5$ consisting of eigenvectors for that matrix?

The End

ALGEBRA PRELIM Monday, March 24, 1986

DIRECTIONS: Do as many problems as you can. Try for complete solutions. All rings have an identity 1, and all modules are unital ($1x = x$).

1. Suppose G is a nilpotent group of order $p_1 p_2 \cdots p_n$, where the p_i are distinct primes. Show that G is cyclic.

2. Let G be a finite p-group, H a subgroup of index p. Show that H is normal in G.

3. Suppose R is a principal ideal domain and x is a nonzero element of R. Show that the Jacobson radical of $R/(x)$ is zero if and only if x is square-free. (Here (x) is the ideal generated by x and <u>square-free</u> means that x factors as a product of <u>distinct</u> primes.)

4. Let M be a finitely generated module over a commutative Noetherian ring R, and let $\varphi : M \to M$ be a homomorphism of R-modules. Show that if φ is onto, then φ is an isomorphism. Give an example showing that this assertion is false if one does not assume M is finitely generated.

5. Show that if A is an $n \times n$ orthogonal matrix over $\mathbb{R}$ (i.e. $AA^T = I$, where A^T is the transpose of A), then $\det(I-A) \geq 0$. (I is the identity matrix.)

6. Suppose K is a field and E is a separable algebraic extension of K. Assume that there is an integer n such that for all $\alpha \in E$, the degree of the minimal polynomial $p_{\alpha,K}$ is less than or equal to n. Show that $\dim_K E$ is finite.

7. Let E be an algebraic extension of the field $\mathbb{F}_p$ (the field with p elements, p a prime), and assume that for every integer $n \geq 1$, E contains a subfield with p^n elements. Show that E is algebraically closed.

Autumn 1985

ALGEBRA PRELIM

Directions: Do as many problems as you can. Try for complete solutions.

1. Let $\mathbf{C}$ be the field of complex numbers, and let $\mathbf{C}[x, y]$ be the ring of polynomials in two variables. Using the fact that every chain of prime ideals in $\mathbf{C}[x, y]$ has at most three terms, prove that a non-maximal, non-zero prime ideal in $\mathbf{C}[x, y]$ is principal.

2. Let A and B be commuting complex $n \times n$-matrices, which are unitary. Show that there is a unitary matrix S and diagonal matrices D_1 and D_2 such that $A = S^{-1}D_1S$ and $B = S^{-1}D_2S$.

3. Let G be a group with $p^m q^n$ elements, where p and q are distinct primes. Show that if $p^t \not\equiv 1 \ mod\ q$ for $t = 1, 2, \ldots, m$, then G has a unique q-Sylow subgroup.

4. Let H be a normal subgroup of a group G. Let G act on a set X.

(a) Show that there is a natural action of G on the set $\overline{X}$ of H-orbits in X.

(b) Show that G acts transitively on X if and only if G acts transitively on $\overline{X}$.

5. Let F be a field, and let $p(x)$ be an arbitrary irreducible <u>cubic</u> polynomial over F. Let G be the galois group of the splitting field of $p(x)$ over F.

(a) If F is the field of rational numbers, list all possibilities for the group G, and give a specific example of a $p(x)$ with each possible galois group. Justify your answers.

(b) If F is a finite field, list all possibilities for G. Explain.

6. Let ξ be a primitive p-th root of unity (p a prime), and let $K = \mathbf{Q}(\xi)$ be the extension of the rational numbers obtained by adjoining ξ.

(a) Find $Tr(\xi^j)$ for any j, where Tr is the trace from K to $\mathbf{Q}$.

(b) Suppose that $\alpha \in K$, and for each j prime to p you know $a_j = Tr(\xi^j \alpha)$. Express α in terms of the a_j and powers of ξ.

7. Let $A = \mathbf{R}[X, Y]/(X - 3Y + Y^3)$ (i.e., the quotient of the real numbers adjoin two indeterminates by the principal ideal generated by $X - 3Y + Y^3$). For $a \in \mathbf{R}$, let I_a be the ideal of A generated by $x - a$. Describe how I_a factors into a product of prime ideals for various values of a.

ALGEBRA PRELIM Spring 1985

Directions: Do as many of the problems as you can. Try for complete solutions.
$\mathbb{Q}$ = field of rational numbers
$\mathbb{R}$ = field of real numbers
$\mathbb{C}$ = field of complex numbers

1. Let G be a simple group which has a subgroup of index n. Show that G is finite and that the order of G divides $n!$.

2. Let N be a group such that (a) every automorphism of N is inner (b) the center of N is trivial. If N is a normal subgroup of a group G, show that $G = H \times N$, where H is the centralizer of N in G.

3. Prove the existence of an irreducible polynomial over $\mathbb{Q}$ of degree 14 whose splitting field over $\mathbb{Q}$ is of degree 14 over $\mathbb{Q}$.

4. Let K be a field, F a subfield of K. Let $a \in K$. If a is algebraic over F, show that $F[a] = F(a)$. If a is not algebraic over F, show that this is false.

5. Give two examples of integral domains in which every nonzero prime ideal is maximal. Give an example in which this is not true. Justify your answers.

6. Determine up to isomorphism all noncommutative semisimple algebras over $\mathbb{R}$ of dimension 6. In each case, determine the number of nonisomorphic simple modules and determine their dimensions over $\mathbb{R}$. <u>Hint</u>: The only finite dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$ and the quaternions $\mathbb{H}$.

7. Let $GL_2(\mathbb{C})$ be the group of invertible 2×2 matrices over $\mathbb{C}$. Show that any finite abelian subgroup of $GL_2(\mathbb{C})$ is isomorphic to a subgroup of $\mathbb{C}^* \times \mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers.

8. Let V be a finite dimensional vector space over $\mathbb{R}$. Suppose that $T: V \longrightarrow V$ is a linear transformation such that $T^2 = -I$ (where I is the identity linear transformation). Show that the dimension of V is even.

ALGEBRA PRELIM Autumn 1984

Directions: Do as many problems as you can. Try for complete solutions.
$\mathbb{Q}$ = field of rational numbers.

1. a) Show that a group of order 160 is not simple.
   b) Show that a group of order 32 is not simple.

2. Let D_n be the dihedral group of order $2n$ (Generators R,H and relations $R^n = I$, $H^2 = I$, and $RH = HR^{n-1}$)
   a) Find the center of D_n.
   b) Describe D_n as the group of symmetries of a geometric figure and then describe the center of D_n geometrically.

3. k^n = n-dimensional space over a field k; $k[x_1,\ldots,x_n]$ = polynomial ring in n-variables over k. Let $P_1,\ldots,P_m$ be m points in k^n and let J be the ideal of elements in $k[x_1,\ldots,x_n]$ which are zero at $P_1,\ldots,P_m$. Show that $k[x_1,\ldots,x_n]/J$ is isomorphic as a ring to the direct product of m-copies of the ring k.

4. Which of the following rings are semisimple? Give some account.
   a) $\mathbb{Q}[x]/(x^4 + 2x^2 + 1)$
   b) $\mathbb{Q}[x]/(x^4 - 2x^2 + 3)$
   c) The ring of matrices $\left\{ \begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & e & f \end{pmatrix} \middle| \text{ entries in } \mathbb{Q} \right\}$.

5. Describe the Galois groups of the following polynomials over $\mathbb{Q}$. Give some reasoning.
   a) $x^3 - 3x + 6$.
   b) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

ALGEBRA PRELIM

Mon. March 19, 1984

Directions: Do as many problems as you can. Try for complete solutions. All rings have an identity 1, and all modules are unital ($1x = x$).

1. Show that if a ring R has exactly one maximal left ideal, then the set of non-units in R is an ideal.

2. Let M be a module over a principal ideal domain R. Suppose that p is a prime element of R, A is a submodule of M, $x \in M$, $x \notin A$, and $px \in A$. Suppose that $\phi: A \longrightarrow B$ is a homomorphism such that $\phi(px) \in pB = \{py \mid y \in B\}$. Show that ϕ extends to a homomorphism $\bar{\phi}: A + xR \longrightarrow B$.

3. Let K be the splitting field of $x^4 - 2$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Draw a diagram of all subgroups of G, indicating which are contained in which. Also draw the corresponding diagram of fields. The fields should be described explicitly (e.g., $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha,\beta)$), and the group elements should also be defined explicitly (i.e., how they act on generators of K). In your diagram of fields, circle <u>all</u> normal extensions of $\mathbb{Q}$. Next, give a geometrical interpretation of G in terms of symmetries of a simple geometric figure. Finally, prove that G is <u>not</u> isomorphic to the quaternion group ($= \{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = -1$ and $ij = k$).

4. (a) Prove that a <u>normal</u> extension of $\mathbb{Q}$ of odd degree must be contained in $\mathbb{R}$.
   (b) Give an example of a <u>normal</u> degree 3 extension of $\mathbb{Q}$. Write your answer in the form $\mathbb{Q}(\alpha)$ with α a specific real number.

5. Let $GL_2(\mathbb{Z})$ denote the group of all invertible 2×2 matrices with integer entries. Let $SL_2(\mathbb{Z}) \subset GL_2(\mathbb{Z})$ consist of all such matrices with determinant 1. Let N be an integer greater than 1. Define $\Gamma_0(N)$ to be the group of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ for which $N \mid c$. Define $\Gamma(N)$ to be the group of all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ for which $a \equiv d \equiv 1 \bmod N$ and $b \equiv c \equiv 0 \bmod N$. Prove or disprove each of the following assertions:
   (a) $SL_2(\mathbb{Z})$ is a normal subgroup of $GL_2(\mathbb{Z})$;
   (b) $\Gamma_0(N)$ is a normal subgroup of $SL_2(\mathbb{Z})$;
   (c) $\Gamma(N)$ is a normal subgroup of $GL_2(\mathbb{Z})$;
   (d) $\Gamma(N)$ is a normal subgroup of $\Gamma_0(N)$ with $\Gamma_0(N)/\Gamma(N)$ solvable.

Let V be a finite-dimensional vector space over $\mathbb{C}$ and let G be a solvable group of linear transformations of V. If each g in G has only 1 as eigenvalue, show that V has a vector v fixed by every transformation in G. (Show this for G abelian first.)

7. Let A and B be $n \times n$ matrices with coefficients in some field k. Show that if $A^2 = A$, $B^2 = B$, and Rank A = Rank B, then A is similar to B.

8. Let A be a ring and L a left ideal.

a) For x and b in A, show that the following two sets are left ideals:

1) $Lx = \{ax \mid a \in L\}$. 2) $\{a \in L \mid ab = 0\}$.

b) Suppose that L is a minimal left ideal in A, and that $L^2 \neq (0)$. Show that L contains an idempotent $e \neq 0$.

ALGEBRA PRELIM

Autumn 1983

Directions: Do as many problems as you can. Try for complete solutions. All rings and algebra have identity and all modules are unital left modules.

1. Let R be a ring, M an R-module. Let $I = \mathrm{Ann}(M) = \{r \in R \mid rm = 0 \text{ for all } m \in M\}$.

   (a) Prove that I is a two-sided ideal of R.

   (b) Prove that if R/I is finite (as a set) and if M is finitely generated as an R-module, then M is finite.

   (c) Prove conversely that if M is finite, then R/I is also finite.

2. Let K^n be the space of column vectors over a field K, and let $M_n(K)$ be the space of $n \times n$ matrices over K. Let A^T be the transpose of an element A of $M_n(K)$ (the ij^{th} entry of A^T is the ji^{th} entry of A). Let x^T be the transpose of an element x of K^n (x^T is a row vector). Let $\langle\ ,\ \rangle$ be the bilinear form on K^n given by: $\langle x,y\rangle = x^T \cdot y$ (matrix multiplication of x^T and y).

   (a) Show that $\langle Ax,y\rangle = \langle x,A^T y\rangle$. $\langle Ax,y\rangle = \langle A(x)^T, y =$

   (b) Show that A has the property $\langle Ax,Ay\rangle = \langle x,y\rangle$ for all x,y in K^n if and only if $A^T = A^{-1}$.

3. Let A be an algebra (with unit) over a field K, and let T be an A-module which is finite-dimensional over K.

   Show that if T has a unique maximal proper submodule, then T is a cyclic module. Does the converse hold? Explain.

4. Let G be a group of order $224 (= 7 \cdot 32)$. Show that G has a proper, normal subgroup.

5. Let G be a finite p-group, where p is a prime. Let C be the center of G, G^1 the commutator subgroup of G. Assume $CG^1 = G$. Prove that G is abelian.

6. Let $\mathbb{Q}$ be the field of rational numbers, and let $k = \mathbb{Q}(\zeta)$, where ζ is a primitive nth root of unity. Let a be an element of k and α a root of $x^n - a = 0$. Let $K = k(\alpha)$.

   (a) Describe the roots of $x^n - a = 0$ in K.

   (b) Show that K/k is Galois.

   (c) Show that the Galois group $\mathrm{Gal}(K/k)$ is cyclic.

7. Let A be a finite-dimensional algebra (with unit) over a field K. Show that A has only a finite number of isomorphism classes of simple left A-modules.

8. (a) Prove that $I = (5, X^2 + 2)$ is a prime ideal in $\mathbb{Z}[X,Y]$ and that $\mathbb{Z}[X,Y]/I$ is a P.I.D.

   (b) Give an explicit example of a maximal ideal of $\mathbb{Z}[X,Y]$ which contains I. (Give a set of generators for such an ideal.)

   (c) Show that there are infinitely many distinct maximal ideals in $\mathbb{Z}[X,Y]$ which contain I.

ALGEBRA PRELIM

Spring 1983

Directions: Do as many of the problems as you can. Complete solutions are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on. But use common sense: do not write a book when a few lines would do. Neatness counts--illegible exams will not be treated charitably.
You should not re-prove major theorems, but if you do use a major result (e.g. the Sylow theorems, Hilbert's basis theorem,...) it would be best to mention it. In this exam, all rings have identity and all modules are unital left modules.

$V^* = \dim_k(V, k)$

1. Let A be an abelian group such that $12a = 0$ for all $a \in A$. Let ✓ $B = \{a \in A : 4a = 0\}$ and $C = \{a \in A : 3a = 0\}$. Show that $A = B \oplus C$.

2. Let V be a finite dimensional vector space over a field k. Let S be a subset of the dual vector space V^*. Let

$$W = \{v \in V : \lambda(v) = 0 \text{ for all } \lambda \in S\}.$$

Suppose that $\mu \in V^*$ and that μ vanishes on W. Show that μ belongs to the linear span of S.

3. Let k be a field and let A be a finite dimensional k-algebra. Let $a \in A$ and define a k-linear map $L_a : A \to A$ by the equation $L_a(x) = ax$ for $x \in A$. Show that a is invertible in A if and only if $\det(L_a) \neq 0$.

4. Let R be a commutative ring. Show that the following two properties that R might have are equivalent. (Think of them as saying that R is "almost" a principal ideal ring.)

   (i) For every nonzero ideal I of R, R/I is a principal ideal ring.

   (ii) If I is an ideal of R and x is a nonzero element of I then there is an element $y \in I$ such that $I = (x, y)$.

5. (i) Let G be a group and N a normal subgroup. Show that there is a homomorphism $\phi: G \to \mathrm{Aut}(N)$ (where $\phi(g)$ takes n to gng^{-1} whose kernel K can be identified with

$$K = \{g \in G: gn = ng \text{ for all } n \in N\}.$$

(Note that $K \cap N = \mathrm{Center}(N)$.)

(ii) Let G be an infinite group and N a finite normal subgroup such that $\mathrm{Center}(N) = 1$. Suppose that G/N is Abelian. Show that G has an Abelian normal subgroup of finite index.

6. Let G be a non-abelian group of order p^3, where p is a prime number. Show that the center Z of G has order p and that G/Z is isomorphic to $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

7. Let A be an algebra over the field $\mathbb{C}$ of complex numbers, (do not assume that A is finite dimensional or commutative).

Let M and N be simple finite dimensional (over $\mathbb{C}$) A-modules.

Let $I_M = \{a \in A: am = 0 \text{ for all } m \in M\}$ and $\{I_N = a \in A: an = 0 \text{ for all } n \in N\}$.

Prove that $M \cong N$ if and only if $I_M = I_N$.

8. Let Q be the field of rational numbers and

$$R = Q[\ldots, x_{-1}, x_0, x_1, x_2, \ldots]$$

the ring of polynomials over Q in an infinite number of variables, where the variables are indexed by integers. Let K be the fraction field of R. Define automorphisms σ and τ of K by defining them first on R as follows: $\sigma(x_i) = x_{i+1}$ $(i \in \mathbb{Z})$, and $\tau(x_i) = x_{-i}$ $(i \in \mathbb{Z})$.

(a) Show that the group generated by σ and τ is noncommutative and has an infinite number of elements of order two.

(b) Show that K has two subfields L and M such that $[K:L] = [K:M] = 2$ but $[K:L \cap M]$ is infinite.

ALGEBRA PRELIM -- AUTUMN 1982

Directions: Do as many problems as you can. Try for complete solutions. The problems ask you to work with algebraic objects; they do not require much specific knowledge.

1. a) Let G_1, G_2 be two non-isomorphic simple groups. Show that the only normal proper subgroups of $G_1 \times G_2$ are $N_1 = G_1 \times id_{G_2}$ and $N_2 = id_{G_1} \times G_2$.

   b) Show that the conclusion of a) is false if $G_1 \simeq G_2 \simeq \mathbb{Z}/(p)$, p a prime.

   c) If $G_1 \simeq G_2$ are non-abelian simple groups, show that the conclusion of a) holds true.

2. Let K/F be a Galois field extension with Galois group D_n, the dihedral group of order $2n$. Which subfields of K are Galois over F? (Give each such subfield as the fixed field of a particular subgroup of D_{2n}.) Also, give the degrees of these extensions of F.

3. Let $S \supset T \supset R$ be commutative K-algebras, K a field. Assume that R is a finitely generated K-algebra, and that S is a finitely generated R-<u>module</u>. Show that T is a finitely generated K-algebra. (First explain why R is Noetherian.)

4. a) Let G be an abelian group. Suppose that N is a subgroup of G such that G/N is infinite cyclic. Show that G contains a subgroup H such that $G = H \times N$.

91

4. b) Is the conclusion of a) true if G/N is just cyclic? Prove this or give a counterexample.

5. Let $\mathbb{R}$, $\mathbb{C}$ be the real and complex numbers. Consider $\mathbb{C}$ as a real vector space with basis $1, i$. The ring $\mathrm{End}_{\mathbb{R}}(\mathbb{C})$ of $\mathbb{R}$-linear transformations of $\mathbb{C}$ can be identified with the ring $M_2(\mathbb{R})$ of real 2×2 matrices, via the basis $1, i$. Let $\rho: \mathbb{C} \to \mathrm{End}_{\mathbb{R}}(\mathbb{C}) = M_2(\mathbb{R})$ be the ring injection $\rho(z)$ = multiplication by z.

   a) Describe the image $\rho(\mathbb{C})$ in $M_2(\mathbb{R})$.

   b) What are the eigenvalues of $\rho(z)$?

   c) For which elements z of $\mathbb{C}$, is $\rho(z)$ a diagonalizable matrix?

6. Let D be a simple ring which contains the real numbers $\mathbb{R}$ in its center.

   a) Give two non-isomorphic simple rings D such that $\dim_{\mathbb{R}}(D) = 16$.

   b) What are the irreducible modules for your examples in a)?

   c) Is there a simple ring D such that $\dim_{\mathbb{R}}(D) = 16$ and the center of D is the complex field?

7. Let B and C be real $n \times n$ commuting symmetric matrices. Show that the equation $X^2 + BX + C = 0$ will have a solution X in the ring of complex $n \times n$ matrices.

8. a) Determine all finitely generated subgroups of $\mathbb{Q}$, the additive group of rationals.

   b) Show that there are infinitely many distinct subgroups of $\mathbb{Q}$ which are not finitely generated.

   c) Show that any two non-trivial subgroups of $\mathbb{Q}$ have a non-trivial intersection.

ALGEBRA PRELIM

9:30-12:30
Mon. March 22, 1982

Directions: Do as many problems as you can. Try for complete solutions. The problems ask you to work with algebraic objects; they do not require much specific knowledge.

1. (i) Show that if $n \geq 6$ and G is a subgroup of A_n of index n (where A_n is the alternating group of degree n), then $G \cong A_{n-1}$.

   (ii) Let G be a finite group and p the smallest prime dividing the order of G. Show that a normal subgroup N of order p is contained in the center of G.

2. Let $F \subset K$ be a Galois extension of fields with Galois group G. By an intermediate field, we mean a field L with $F \subset L \subset K$, and we call L proper if $L \neq F$ and $L \neq K$.

   (i) If $|G| = 30$, what can you say about the existence and dimensions of proper intermediate fields which are Galois extensions of F?

   (ii) Construct an example of a Galois extension $F \subset K$ for which there are proper intermediate fields, but such that none of these intermediate fields are Galois over F.

Let S be a commutative ring and R a subring, and suppose that there are elements $\alpha_1, \ldots, \alpha_n$ in S such that every element of S can be written (possibly non-uniquely) as a polynomial in the elements α_i, where the coefficients of the polynomial are in R. Suppose that for each i, there is a monic polynomial $f_i(t)$ in $R[t]$ such that $f_i(\alpha_i) = 0$.

   (i) Show that S is finitely generated as an R-module.

   (ii) Assume that R is Noetherian, and prove that for every $s \in S$, there is a monic polynomial $g(t)$ in $R[t]$ such that $g(s) = 0$.

4. Let D be a noncommutative division ring, and $D[x]$ the ring of polynomials in one (commuting) variable over D.

   (i) Show that if I is a left ideal in $D[x]$, and if f is a monic polynomial of smallest degree in I, then I is generated by f as a left ideal. (That is, $I = D[x]f$.)

   (ii) Show that if I is a two-sided ideal, and f is a monic polynomial of smallest degree in I, then f generates I as a left ideal and as a right ideal, and for every $\alpha \in D$, there is a $\beta \in D$ with $\alpha f = f\beta$.

   (iii) (continuing (b)) Show that the coefficients of f are all in the center of D.

5. Let R be a ring (with 1) and let M be the ring R regarded as a <u>right</u> module over itself.
   (i) What are the submodules of M?
   (ii) If I is a right ideal of R, let $S_I = \{r \in R: rI \subseteq I\}$. Show that S is a subring of R, that I is a two-sided ideal of S, and that S is the largest subring of R containing I as a two-sided ideal.
   (iii) Show that for any $s \in S$, the map taking x to sx is an endomorphism of M which takes I into itself. (Remember, M is R viewed as a <u>right</u> R-module.)
   (iv) Show that $S/I \cong \mathrm{End}(M/I)$, (isomorphism of rings.)

6. Let G be an Abelian group (not necessarily finitely generated) and A and A' subgroups. Prove or give a counterexample for each of the following.
   (i) $A \cong A'$ implies $G/A \cong G/A'$.
   (ii) $G/A \cong G/A'$ implies $A \cong A'$.
   (iii) If $G = A \oplus B = A' \oplus B'$ and $A \cong A' \cong \mathbb{Z}$, then $B \cong B'$.
   (Hint: if $B \neq B'$, show $B \cong (B' \cap B) \oplus \mathbb{Z}$.)

7. Let E be the usual 3-dimensional, real, Euclidean space with the usual norm. A linear transformation $T: E \to E$ is a <u>rigid motion</u> if (i) $|T(x)| = |x|$ for all $x \in E$, and (ii) $\det(T) = 1$. Show that if T is a rigid motion, then there is a nonzero vector v such that $T(v) = v$. (Hint: first consider what real eigenvalues T can have.)

8. All matrices in this problem are over the complex numbers.
   (i) Compute the characteristic and minimal polynomials of the following matrices (assuming $\alpha \neq \beta$).

   a) $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$ b) $\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$

   (ii) What are necessary and sufficient conditions on a pair of polynomials, $M(x)$ and $F(x)$, for there to be a matrix T such that $M(x)$ is the minimal polynomial of T and $F(x)$ is the characteristic polynomial of T? (Prove your answer is correct.)
   (iii) Prove or disprove: two diagonal $n \times n$ matrices with the same <u>minimal</u> polynomial are similar.

ALGEBRA PRELIM

9:30 - 12:30
Mon. Sept. 14, 1981

Directions: Do as many problems as you can. Try for complete solutions. The problems ask you to work with algebraic objects; they do not require much specific knowledge.

1. Let $\mathbb{R}$ denote the field of real numbers.
   (a) Prove that $\mathbb{R}[X]$ is a principal ideal domain.
   (b) Show that there is a one-to-one correspondence between the reduced ideals of $\mathbb{R}[X]$ (those that are their own radical) and finite subsets S of the complex plane having the property that $x \in S \Longrightarrow \bar{x} \in S$.
   (c) Under this correspondence, what subsets do the prime ideals correspond to?

2. Let A and B be linear transformations of an n-dimensional vector space V over a field F.
   (a) If A and B commute, show that B transforms each characteristic subspace for A into itself.
   (b) If A and B commute and are (separately) diagonalizable, show that there is a basis for V which diagonalizes A and B simultaneously.
   (c) Show that any m commuting diagonalizable linear transformations of V may be diagonalized simultaneously.

3. Let R be a ring. Let M be an R-module which is the direct sum $\oplus M_i$ of simple R-submodules M_i, where no two M_i are isomorphic R-modules. Show that each submodule N of M has the property:

$$N = \oplus (M_i \cap N).$$

4. Let F be a field. Let α be an automorphism of F of order 2, and let b be an element of the fixed field of α. Let $F + F\cdot x$ be a two-dimensional F-vector space with (associative, non-commutative) ring structure determined by $x^2 = b$ and $x\cdot c = \alpha(c)\cdot x$ for all $c \in F$. In terms of this data, give necessary and sufficient conditions for $F + Fx$ to be a division ring.

5. Let G be a finite group, let C^* be the multiplicative group of nonzero complex numbers, and let $\hat{G}$ be the set of all homomorphisms from the group G to the group C^*.
   (a) Prove that $\chi(g)$ is a root of unity for all $\chi \in \hat{G}$ and all $g \in G$.

(continued on next page)

5. (continued)

(b) For any fixed $\chi \in \hat{G}$, let $S(\chi)$ denote $\sum_{g \in G} \chi(g)$. Show that for any $\chi \in \hat{G}$ and any $g \in G$:

$$S(\chi) = \chi(g)\, S(\chi).$$

Then prove that

$$S(\chi) = \begin{cases} \#G & \text{if } \chi \text{ is the trivial homomorphism,} \\ 0 & \text{otherwise.} \end{cases}$$

(c) Now suppose that G is abelian. Prove that:

(i) $\#\hat{G} = \#G$;

(ii) for every element $g \neq$ the identity e, there exists $\chi \in \hat{G}$ such that $\chi(g) \neq 1$;

(iii) for fixed $g \in G$:

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} \#G & \text{if } g = e, \\ 0 & \text{otherwise.} \end{cases}$$

6. Prove that the ideal $(2, 1+\sqrt{-3})$ in the ring $R = Z[\sqrt{-3}]$ is a proper ideal, a prime ideal, and <u>not</u> a principal ideal. Now let $\omega = (1+\sqrt{-3})/2$. Use the Euclidean algorithm to prove that all ideals in $Z[\omega]$ are principal.

7. Let $Q[X_1,\ldots,X_n]$ be the polynomial ring in n variables over the field Q of rational numbers, and let S_n be the symmetric group of permutations of $\{1,\ldots,n\}$. Let S_n operate on $Q[X_1,\ldots,X_n]$ as follows: for $\sigma \in S_n$ and $f \in Q[X_1,\ldots,X_n]$, $(\sigma f)(X_1,\ldots,X_n) = f(X_{\sigma(1)},\ldots,X_{\sigma(n)})$ (i.e., replace the variable X_i in f by $X_{\sigma(i)}$). Note that $\sigma(fg) = \sigma(f)\,\sigma(g)$.

(a) Show that $\sigma\left(\prod_{i<j} (x_i - x_j)^2\right) = \prod_{i<j} (x_i - x_j)^2$, and conclude that $\sigma\left(\prod_{i<j} (x_i - x_j)\right) = \pm \prod_{i<j} (x_i - x_j)$.

(b) Let $\operatorname{sgn}\sigma \in \{\pm 1\}$ be determined by: $\sigma\left(\prod_{i<j} (x_i - x_j)\right) = (\operatorname{sgn}\sigma) \prod_{i<j} (x_i - x_j)$.

Show that $\operatorname{sgn}\sigma = -1$ if σ is the transposition $(i, i+1)$.

(c) Prove that $\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}$ is a homomorphism from the group S_n to the group of two elements.

8. Let K be the field extension of the rational numbers Q obtained by adjoining a primitive N-th root of unity.

(a) What is the Galois group of K over Q?

(b) If $N = 56$, how many different fields F exist such that (i) $Q \subseteq F \subseteq K$?

(ii) $Q(\sqrt{2}) \subseteq F \subseteq K$?

<u>end of exam</u>

ALGEBRA PRELIM March 1981

Directions: Complete solutions to the following problems are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on. But use common sense! Do not write a book when a few lines would do. Neatness counts. Do as many of the problems as you can.

1. Let G be a finite simple group of order ≥ 3. Prove that G is isomorphic to a subgroup of A_n if and only if G has a proper subgroup of index $\leq n$. (A_n denotes the alternating group on n letters.)

2. Let G be a finite group. Which of the following statements are true? Provide proofs or counterexamples.

   (a) Let N be a normal subgroup of G and let p be a prime number which divides $|G|$, but which does not divide $|G/N|$. Then every Sylow p-subgroup of G is contained in N.

   (b) Let p be the largest prime which divides $|G|$. Then the number of elements x of G satisfying $x^p = 1_G$ is a divisor of $|G|$.

   (c) Assume that $G = G_1 \times G_2$ (a direct product of subgroups G_1, G_2). Let H be a subgroup of G. Then $H = H_1 \times H_2$, where $H_1 = G_1 \cap H$ and $H_2 = G_2 \cap H$.

3. Let E be an infinite dimensional vector space over a field k. Let $\mathrm{End}_k(E)$ be the ring of k-linear transformations from E to E. Show that $\mathrm{End}_k(E)$ is not simple. (Hint: Find a proper two-sided ideal in $\mathrm{End}_k(E)$.)

4. Let K be an algebraic extension of k (not necessarily finite-dimensional over k.) Let G be the group of automorphisms of K over k. For $\alpha \in K$, let $G_\alpha = \{\sigma \in G \mid \sigma(\alpha) = \alpha\}$.

   (a) Show that the index $[G:G_\alpha]$ is finite.

   (b) Let K^G = fixed field for $G = \{\beta \in K \mid \sigma(\beta) = \beta \ \forall \sigma \in G\}$. Show that K is a separable and normal extension of K^G.

5. Let E be a field extension of F. Let K and L be finite extensions of F contained in E such that $K \cap L = F$. Let KL denote the subfield of E generated by K and L.

   (a) Assume that K is Galois over F. Prove that KL is Galois over L and that there is a group isomorphism $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/F)$.

   (b) If K/F is Galois, show that $[KL:F] = [K:F][L:F]$.

   (c) If K/F is not Galois, is it necessarily true that $[KL:F] = [K:F][L:F]$?

6. Let R be a ring with identity.

   (a) Show that an R-submodule of a semisimple R-module E is also semisimple.

   (b) Let $\mathrm{Rad}(R)$ = intersection of all maximal left ideals of R. If R is left Artinian and $\mathrm{Rad}(R) = (0)$, prove that R is a semisimple ring (i.e., R is a semisimple R-module under left multiplication).

7. Let $R = F[X]$ be the polynomial ring in one variable over a field F. (Assume that F is infinite.)

   (a) Prove that R is a principal ideal domain.

   (b) Let M be a cyclic torsion R-module. (M is torsion means that for each $m \in M$, there is a nonzero element $r_m \in R$ such that $r_m \cdot m = 0$. M is cyclic means that there is an element $m \in M$ such that $M = Rm$.) Prove that M has only finitely many R-submodules.

7. (Continued)

(c) Is the conclusion of (b) true for every finitely generated torsion R-module? Provide a proof or a counterexample.

(d) Let $S = F[X,Y]$ be the polynomial ring over F in two variables. Let M be a cyclic torsion S-module. Must M have only finitely many S-submodules? Provide a proof or counterexample.

8. Let A be an $n \times n$ matrix with entries in a field F. Consider the F-linear transformation $T_A : M_n(F) \to M_n(F)$ defined by $T_A(B) = AB - BA$ for B in $M_n(F)$. Assume that the characteristic polynomial for A has n distinct roots in F. Prove that $\text{rank}(T_A) = n^2 - n$.

ALGEBRA PRELI Autumn 1980

Directions: Do any five of the following problems.

1. Let p,q,r $(p < q < r)$ be primes and let G be a group of order pqr.

(a) Show that G is solvable.

(b) Must G be nilpotent?

2. Show that a minimal normal subgroup of a finite solvable group is an abelian group in which every element has order p for some prime p.

3. Determine the Jacobson radical of each of the following.

(a) The ring of all 3x3 lower triangular matrices with entries from a field.

(b) The ring $Q[x]/I$, where Q is the field of rational numbers and I is the ideal generated by $(x^2 + 1)^6$.

(c) The ring $F[x]/I$, where F is the field with p elements and I is the ideal generated by $x^p - 1$.

4. Let R be a commutative ring with identity, I an ideal of R and S a non-empty multiplicatively closed subset of R such that $I \cap S = \emptyset$. Show that R has a prime ideal P such that $P \supseteq I$ and $P \cap S = \emptyset$.

5. Let V be a finite dimensional vector space over a field of characteristic 0 and let B be a non-degenerate skew-symmetric ($B(x,y) = -B(y,x)$) bilinear form on V. For U a subset of V, let

$$U^{\perp} = \{ v \in V \mid B(u,v) = 0 \text{ for all } u \in U \}.$$

(a) Let U be a subspace of V. Show that $\dim U + \dim U^{\perp} = \dim V$.

(b) Show that V has a subspace W with $W = W^{\perp}$.

6. Let E be a finite dimensional Galois extension of a field K and let $a \in E$. Let A be the K-linear transformation of E given by $Ab = ab$. Show that $\text{trace}(A) = \sum_{g \in G} g(a)$, where G is the Galois group of E/K.

7. Let E be an algebraic extension of a field K and let $g: E \to E$ be a field homomorphism such that $g(k) = k$ for all $k \in K$. Show that g is an automorphism of E. (E is not assumed to be finite dimensional over K.)

8. Let K be a field of characteristic 0 and let $f(x) \in K[x]$ be an irreducible polynomial of prime degree. Let L be a splitting field for $f(x)$ over K. Show that the Galois group of L/K is nilpotent if and only if it is cyclic.

9. Describe the Galois group for each of the following polynomials over the field of rational numbers.

(a) $x^7 - 2$

(b) $x^6 - 2$

(c) $x^5 - 5x + 1$

ALGEBRA PRELIM Spring 1980

Directions: Do as many of the problems as you can. Complete solutions are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on. But use common sense: do not write a book when a few lines would do. Neatness counts--illegible exams will not be treated charitably. You should not re-prove major theorems, but if you do use a major result (e.g. the Sylow theorems, Hilbert's basis theorem,...) it would be best to mention it. In this exam, all rings have identity and all modules are unital left modules.

1. Let V be a vector space. Define a canonical homomorphism $V \to V^{**}$ (where "*" means "dual"), and show (a) that it is always injective, and (b) that it is an isomorphism if V is finite dimensional.

2. Show that a group of order 150 has a normal subgroup of order 5 or 25.

3. Let V be a finite dimensional vector space and T and S linear transformations of V into itself, such that $\mathrm{Ker}(S) = \mathrm{Ker}(T)$. Show that there is an invertible linear transformation U such that $UT=S$. (We regard linear transformations as acting on the left of V.)

4. If A is a module over a ring R, the annihilator of A, written $\mathrm{Ann}(A)$, is defined by

$$\mathrm{Ann}(A) = \{r \in R : ra = 0 \text{ for all } a \in A\}.$$

A module A is called critical if it is nonzero and $\mathrm{Ann}(A) = \mathrm{Ann}(A')$ for every nonzero submodule A' of A.

(a) Show that if R is commutative and A is a critical R-module then $\mathrm{Ann}(A)$ is a prime ideal.

(b) Show that if R is commutative and Noetherian, and B is any nonzero R-module, then B has a critical submodule.

5. Let k be a field; X,Y,Z indeterminates; U,V,W the elementary symmetric functions in X,Y,Z ($U = X+Y+Z$, $V = XY+YZ+ZX$ and $W = XYZ$); $L = k(X,Y,Z)$, $K = k(U,V,W)$. The extension L/K is Galois with Galois group equal to the permutation group on the letters X,Y,Z (you don't need to prove this fact). Let ω be any element of k such that $\omega^3 = 1$. Show that $(X + \omega Y + \omega^2 Z)^3$ is contained in a quadratic extension of K.

6. If A is an Abelian group (written additively) and p is a prime number, we let $pA = \{pa : a \in A\}$. Then A/pA is a $\mathbb{Z}/p\mathbb{Z}$-vector-space, and we let its dimension be $d_p(A)$. In terms of the usual invariants for finitely generated Abelian groups, what does it mean for two finitely generated Abelian groups A and B to have the property that $d_p(A) = d_p(B)$ for all primes p?

7. Let E/F be a field extension and A and B square matrices with entries from F such that there is an invertible matrix S with entries from E such that $SAS^{-1} = B$. Show that there is an invertible matrix T with entries from F such that $TAT^{-1} = B$.

8. (a) What is the Jacobson radical of each of the following rings: (Justify your answer <u>briefly</u>).

   $\mathbb{Z}$ $\qquad$ $\mathbb{C}[[X]]$ (power series in one variable over complex numbers)

   $M_2(\mathbb{R})$ (two by two matrices over the real numbers).

   (b) Are nilpotent elements of a ring R necessarily in the Jacobson radical? Is the answer different if R is commutative? (Justify your conclusions.)

   (c) Are the elements of the Jacobson radical necessarily nilpotent? Is the answer different if R is commutative? (Justify your conclusions.)

9. (a) Let k be an algebraically closed field, let A be a k-algebra (so we have a ring homomorphism $k \to A$ taking 1 to 1, such that the image of k is in the center of A.) Let M be a <u>simple</u> A-module which is finite dimensional over k. Show that the canonical homomorphism $k \to \mathrm{End}_A(M)$ is an isomorphism.

   (b) Give an example of an algebraically closed field k, and a k-algebra A with a module M which is finite dimensional over k, such that M is <u>not</u> simple but such that the natural map $k \to \mathrm{End}_A(M)$ is an isomorphism.

10. Let V be a vector space of dimension 2 over a field k and $\beta: V \times V \to k$ a symmetric, bilinear form.

   (a) Suppose that for some $v \in V$, $\beta(v,v) \neq 0$. Show that V has a basis with respect to which the <u>matrix</u> of β is diagonal. (Reminder: if $\{e_1, e_2\}$ is a basis, then the matrix of β with respect to this basis has entries $b_{ij} = \beta(e_i, e_j)$.)

   (b) Suppose you do not know that there is an element v with $\beta(v,v) \neq 0$, but you know that $\beta \neq 0$. Assuming that the characteristic of k is not 2, show that there <u>is</u> such an element v.

11. Let G be a finite group of order p^n, where p is a prime and n is a positive integer.

   (a) If G acts on a finite set X whose cardinality is not divisible by p, then there exists $x \in X$ such that $g \cdot x = x$ for all $g \in G$.

   (b) The center of G is non-trivial.

   (c) Let V be a non-trivial finite dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$. Suppose that $\rho: G \to \mathrm{Aut}(V)$ is a homomorphism of G into the group of invertible linear transformations of V. Then there exists a non-zero vector $v \in V$ such that $\rho(g)\, v = v$ for all $g \in G$.

ALGEBRA PRELIM

9:30-12:30
Monday, Sept.17/79

Directions: Answer as many of the following problems as you can.

Guideline: seven problems done completely will be considered a very reasonable performance.

1. Prove that any group G of order p^2q^2, where p and q are prime and $p > q \geq 3$, is solvable.

2. (a) If an abelian group G is generated by n elements, then prove that every subgroup of G is generated by n elements. [You may not assume that this theorem is true for free abelian groups].

   (b) Let G be a torsion-free abelian group and let H be a subgroup of G. Prove that G/H is torsion-free if and only if $nG \cap H = nH$ for every positive integer n.

3. Give an example of groups G_1 and G_2 where G_1 is abelian and G_2 is not abelian, but the groups of automorphisms of G_1 and G_2 are isomorphic.

4. Let R be an integral domain which is <u>not</u> a field, having the property that every proper ideal is the product of maximal ideals. Show that

   (a) If M is a maximal ideal of R, then there exists $a \in R$ and an ideal $K \neq \{0\}$ such that $MK = (a)$.

   (b) If I,J,M are ideals of R with M maximal, then $IM = JM$ implies $I = J$.

5. Let R be a ring with a two-sided ideal I. Suppose there exists $e \in I$ such that $ei = ie = i$ for all $i \in I$. Show that there exists a two-sided ideal J of R such that $R = I \oplus J$.

6. (a) Prove that a principal ideal domain satisfies the ascending chain condition on ideals.

   (b) Show that every non-unit in a principal ideal domain is a product of irreducible elements.

7. (a) Assume that $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \in \mathbb{Q}[x]$ has exactly one real root.

Show that the Galois group of $f(x)$ over $\mathbb{Q}$ is either S_2 or S_3.

(b) Find the Galois group of $f(x) = x^3 - x + \frac{1}{3}$ over $\mathbb{Q}$.

(c) Find the degree of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ over $\mathbb{Q}$.

8. Let $K \subset L \subset M$ be fields. Assume $\Theta \in M$ is algebraic over K and that $K(\Theta)$ is Galois over K.

(a) Why is $L(\Theta)$ normal and separable over L?

(b) Show that the Galois group of $L(\Theta)$ over L is isomorphic to the Galois group of $K(\Theta)$ over $K(\Theta) \cap L$.

9. List one representative of each similarity class of the $n \times n$ complex matrices J such that $J^2 = -I_n$, where I_n is the $n \times n$ identity matrix.

10. Suppose that A and B are $n \times n$ matrices over an algebraically closed field such that the $2n \times 2n$ matrices $\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$ and $\begin{bmatrix} B & 0 \\ 0 & B \end{bmatrix}$ are similar.

Show that A and B are similar.

ALGEBRA PRELIM

Spring 1979

1. Prove that in a group G of order 30 each 3-Sylow subgroup is normal, each 5-Sylow subgroup is normal and G has a normal subgroup of order 15.

2. Show that a group of order 80 is solvable.

3. Let a be a positive real number and n an integer greater than 2. Show that the splitting field of $x^n - a$ in the complex field contains a real subfield of index 2.

4) Let p be a prime integer and F_{p^m} the field with p^m elements. For given n and m find all integers t for which there is a non-zero ring homomorphism $F_{p^n} \otimes_{F_p} F_{p^m} \to F_{p^t}$.

For which pairs (n,m) is $F_{p^n} \otimes_{F_p} F_{p^m}$ a field?

5. If R is a ring (perhaps without an identity) and I is a minimal left ideal of R with $I^2 \neq 0$, then $I = Re$ for some idempotent $e \in I$.

6. Let $M(n,F)$ be the ring of $n \times n$ matrices over the field F.
Find all the central idempotent elements in $M(n,F)$.
Show that, for $n \neq m$, $M(n,F)$ and $M(m,F)$ are not <u>ring</u> isomorphic.

7. Prove the following:
If R is a commutative ring with identity and J is an ideal of R such that every non-zero ideal of R is a power of J, then every ideal of R is principal.
If $\bigcap_n J^n = 0$ then there is an $x \in R$ such that each $0 \neq y \in R$ has the form $y = ux^k$ with u a unit.

8. If R is a commutative ring with identity and P is an ideal maximal among the ideals that are not finitely generated, then P is a prime ideal.

9. Suppose V is a finite dimensional vector space over a field F and $T:V \to V$ is linear. Show that there is a positive integer k such that $V = T^k(V) \oplus \mathrm{Ker}(T^k)$.

10. For σ an $n \times n$ complex matrix, $\bar{\sigma}$ is the matrix whose ij-th entry is the conjugate of the ij-th entry of σ and σ^t is the transpose of σ. σ is unitary if $\bar{\sigma}^t = \sigma^{-1}$ and A is Hermitian if $\bar{A}^t = A$.

Explain how a Hermitian matrix may be diagonalized by some unitary matrix.

Show that if B is a real symmetric matrix and σ a unitary matrix such that $\sigma B \sigma^{-1}$ is diagonal, then the entries of $\sigma B \sigma^{-1}$ are real.

ALGEBRA PRELIM AUTUMN 1978

Directions: Do Problem 1 and five (5) of the remaining problems. Complete solutions are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on. But use common sense. Do not write a book when a few lines would do. Neatness counts--illegible exams will not be treated charitably.

1. This problem is required. It has 5 parts. Each is a statement, to be judged true or false, with a short proof or counterexample.

   (i) A finite ring with identity and with no nilpotent elements is commutative.

   (ii) The additive group of the rational numbers has no maximal proper subgroups.

   (iii) If R is a commutative ring and $R[x]$ is Noetherian, then R is Noetherian.

   (iv) Any subgroup of A_6 of index 6 is isomorphic to A_5.

   (v) If A and B are finite Abelian groups of orders n and m, then the tensor product $A \otimes B$ has exactly mn elements.

2. Let G be a group of order 80, which does not have a normal subgroup of order 16. Then G has at least two distinct normal subgroups (other than (1) and G).

3. G is a finite Abelian group with an element x of order 9 such that $G/(x)$ is cyclic of order 9. Up to isomorphism, what are the possibilities for G? (Be sure to specify with each group the element x you would use.)

4. Let V be a finite dimensional vector space and A and B two linear transformations of V into itself such that $A^2 = B^2 = 1$. Show that if $\text{rank}(A-1) = \text{rank}(B-1)$, then A and B are similar. (Here "1" denotes the identity matrix. Hint: first consider fields of characteristic not 2.)

5. Let ξ be a primitive nth root of unity $(n > 2)$. Show that the degree of $Q(\xi+\xi^{-1})$ over Q is $\frac{1}{2}\phi(n)$, where ϕ is the Euler function.

6. Let R be a ring with identity and let I be a minimal right ideal of R. Show that either (a) $I^2 = 0$, or (b) there is a right ideal K of R with $R = I \oplus K$.

7. Let R be a commutative ring with identity in which every non-empty collection of ideals has a minimal element.

(a) Show that every prime ideal of R is a maximal ideal.

(b) Show that R has only a finite number of prime ideals.

8. Let L be a finite normal extension of the field Q of rational numbers and let $f(x) \in Q[x]$ be an irreducible polynomial. Suppose that $f(x) = p_1(x)\ldots p_n(x)$ is a factorization of $f(x)$ into irreducible factors in $L[x]$. Show that the $p_i(x)$ all have the same degree.

9. Let V be a vector space (not necessarily finite dimensional) and s a linear transformation of V into itself. Show that there is a linear transformation t such that $sts = s$. Show that if V is finite dimensional, t may be chosen to be invertible, but that this is false if V is infinite dimensional.

ALGEBRA PRELIM Spring 1978

DO AS MANY PROBLEMS AS YOU CAN THOROUGHLY

1. P a p-Sylow subgroup of a finite group G. Denote the normalizer of a subgroup H of G by N(H). Show that $N(N(P)) = N(P)$.

2. Let q be a prime integer and let p be a prime integer which divides $q - 1$. For each integer $n \geq 1$, construct a non-abelian group of order $p^n \cdot q$.

3. Let G be a group of order n and let H be a subgroup of order m. Suppose that for each $g \in G - H$, $H \cap (g^{-1}Hg) = \{1\}$. Show that there are exactly $\frac{n}{m} - 1$ elements of G which lie in no conjugate of H.

4. Show that the Jacobson radical of a ring with 1 (commutative or not) contains no (non-zero) idempotents.

5. a) Let p be a prime in the ring Z of integers. Denote the localization of Z at the prime ideal (p) by $Z_{(p)}$. Show that $Z_{(p)}$ is not finitely generated as a Z-algebra.

   b) Let R be any commutative Noetherian ring. Show that the localization R_P of R at a prime ideal P is Noetherian.

6. Let M be a finitely generated Z-module (Z = ring of integers). Express $\dim_{F_p} M \otimes_Z F_p$, the dimension of $M \otimes_Z F_p$ over the field F_p with p elements, in terms of the invariants of M as a Z-module (i.e. as an abelian group.)

7. Let M_{nF} be the $n \times n$-matrix ring with entries in a field F. Show that all irreducible (simple), left modules for M_{nF} are isomorphic.

. Let V be a finite-dimensional real inner product space. Suppose that V is the orthogonal direct sum of subspaces W and W'. Let $p_1 : V \to W$ be the projection onto the summand W. Show that, relative to any orthonormal basis for V, p_1 has a symmetric matrix. (Regard p_1 as a linear transformation from V to V.)

9. Let n,m be positive integers. Classify up to similarity all $n \times n$ matrices A over the complex numbers that satisfy the relation $A^m = I$. (I = identity matrix.)

10. a) Let $f(x) = f_1(x)f_2(x)$ be the product of polynomials f_1, f_2 with rational coefficients. Suppose that f_2 is irreducible over the splitting field of f_1. Show that the Galois group of the splitting field of f is the direct product of the Galois groups of the splitting fields of f_1 and f_2. False (see below)

b) What are the Galois groups of $f(x) = (x^2 + 1)(x^2 + 4)$ and of $g(x) = (x^2 + 1)(x^2 + 2)$?

11. Let p be an odd prime integer and a an integer relatively prime to p. Show that the equation $x^2 \equiv a \pmod p$ has a solution in the ring of integers if and only if $a^{(p-1)/2} \equiv 1 \pmod p$.

Counter example for 10a

$f_1 = x^2+1$ Splitting field $Q(i)$

$f_2 = x^4-2$ (roots $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}\,i$) spl. field $Q(\sqrt[4]{2}, i)$

f_2 is irred over $Q(i)$, but

$Q(\sqrt[4]{2}, i)$ is a spl. field of both f_2 and $f_1 f_2$.

If the circled hypothesis is replaced by "the intersection of the splitting fields of f_1 and of f_2 is Q" then the conclusion is true.

ALGEBRA PRELIM AUTUMN 1977

Directions: The exam is divided into four parts. Answer a total of seven questions, at least one in each part, and not more than two in each part. Indicate clearly which seven problems are to be graded (you cannot count two partially done problems as one).

Part I. GROUPS

1. (a) Prove that there is no simple group of order 56.

   (b) If C is the center of a group G and G/C is cyclic, then prove that G is abelian.

2. (a) If $m|n$ and $2 \nmid n$, then prove that the automorphism group of $Z_m \oplus Z_n$ is nonabelian.

   (b) Prove that the automorphism group of a noncyclic finite abelian group (whose order is not divisible by 2) is nonabelian.

3. Prove that the multiplicative group of positive rational numbers is a free abelian group.

4. A subgroup H of G is special if for each pair $x,y \in G$ with $x \notin H$, there is a unique $u \in H$ with $y^{-1}xy = u^{-1}xu$.

   Suppose H is a special subgroup of G. Then show:

   (a) $G = C(x)H$ and $C(x) \cap H = \{1\}$ where $C(x)$ is the centralizer of x in G.

   (b) H is normal in G.

Part II. RINGS AND MODULES

5. Let R be a ring with identity. Assume R has a unique maximal left ideal. Prove that

   (a) R/J is a division ring, where J is the Jacobson radical of R.

   (b) The characteristic of R is either 0 or a prime power.

6. Let R be a principal ideal domain (with identity) that is not a field. Prove that R is Jacobson semisimple if and only if R contains an infinite number of distinct, nonassociate irreducible elements.

7. Let R be a ring with identity with Jacobson radical J.

   (a) Prove that if M is a finitely generated left R-module such that JM = M, then M = 0. [Prove this - don't just quote a famous theorem.]

   (b) Use part (a) to prove that if R is Artinian, then J is nilpotent.

Part III. FIELDS AND GALOIS THEORY

8. (a) Find the Galois group of $x^4 - 2x^2 - 15$ over the field Q of rationals.

   (b) Use the Fundamental Theorem of Abelian Groups to prove that the multiplicative group of a finite field is cyclic.

9. An algebraic closure of a field K is an algebraic extension field F of K such that every polynomial in K[x] has a root in F. Prove that an algebraic extension field F of K is an algebraic closure of K if and only if for every extension field E of a field K_1 and isomorphism $\sigma: K_1 \to K$, σ extends to a monomorphism $E \to F$.

10. For any field E of characteristic $p \neq 0$, let $E^{p^n} = \{u^{p^n} \mid u \in E\}$. E^{p^n} is known to be a subfield of E. If L and M are subfields of E, then LM denotes the smallest subfield of E containing both L and M.

    Let F be a finite dimensional extension field of K, with char $K = p \neq 0$. Assume that $KF^p = F$. Prove that F is separable over K.

    [Hints: Let S be the maximal separable subfield of F. Show that $S = KF^{p^m}$ for some m. Then show that $F = KF^p = KF^{p^2} = \cdots = KF^{p^m}$.]

ALGEBRA PRELIM SPRING 1977

All rings R are commutative with identity.

The parts of this problem are to be answered true or false. If true, give a short proof; if false give a counterexample.

(a) The only field automorphism of the field of real numbers $\mathbb{R}$ is the identity.

(b) Each group in column (A) can be paired with an isomorphic group in column (B). Here, $Z_n = Z/nZ$, $Z_n^\times$ = group of units with respect to multiplication in Z_n, S_n = symmetric group on n letters; and A_n = alternating group on n letters.

(A)	(B)
$Z_5 \times Z_2$	$Z_{15} \times Z_{12}^\times$
$Z_{15}^\times$	$Z_5^\times \times (263Z/526Z)$
$Z_{30} \times Z_2$	$Z_2 \times A_3 \times (S_{20}/A_{20})$
$Z_8^\times \times Z_{15}$	$Z_{11}^\times \times Z_7^\times$
Z_8	$Z_{64}/8Z_{64}$

(c) Let $K = k(x)$ be the field of rational functions in the indeterminate x over the field k. Let $\{f_i \mid i \in I\}$ be the set of all monic irreducible polynomials in $k[x]$. Then $K = k[x][1/f_i]$, $i \in I$.

(d) The group of nonzero rational numbers is a (discrete) direct product of cyclic groups.

(e) If S is a multiplicatively closed subset of a ring R, and $\{A_i\}$ is a collection of ideals of R, then $S^{-1}(\bigcap_i A_i) = \bigcap_i (S^{-1}A_i)$.

(f) If $\phi : M \to M$ is a surjective homomorphism of a noetherian R-module M, then ϕ is an isomorphism

(g) If for every element x in a ring R, there is an integer $n \geq 2$ so that $x^n = x$, then every prime ideal of R is maximal.

(h) Two idempotent linear transformations of a finite dimensional vector space are similar if and only if they have the same rank.

(i) For any field $K \supseteq Q$ and any integer $n \geq 20$, there exist $A, B \in M_n(K)$ such that $AB - BA = 1$.

(j) Let J be the intersection of all maximal ideals in a ring R. Then $x \in J$ if and only if $1 - xy$ is a unit of R for all $y \in R$.

(k) Recall that a local ring is a ring with only one maximal ideal. The only idempotents of a local ring are 0 and 1.

II

1. (a) Let H and K be two subgroups of a group G, each of finite index in G. Prove that $H \cap K$ has finite index in G and give an upper bound for this index.

(b) Using the result of (a), show that if a subgroup H of G has finite index in G, then H contains a normal subgroup of G which has finite index in G.

2. Prove that the polynomial $1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ is irreducible over the field of rational numbers Q, but is reducible over Z_{127}.

3. Find the Galois group of $x^4 + 2 = 0$ over Q, and express this group as a permutation group on the zeros of $x^4 + 2$.

4. (a) Let V be a finite dimensional vector space, and let T be an endomorphism of V. Further, suppose that $V = \bigoplus_i V_i$, where the V_i are T-stable subspaces of V, and that the corresponding projections $V \to V_i$ are polynomials in T. Prove that if W is any T-stable subspace of V, then $W = \bigoplus_i (W \cap V_i)$.

(b) Let $V = C^{(4)}$, where C is the field of complex numbers,

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \text{ and } B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Find all of the subspaces of V that are invariant under both A and B.

(a) Let P be a prime ideal in a commutative ring with identity R. Show that the field of fractions of $R/P \cong R_P/PR_P$, where R_P denotes the localization of R at P.

(b) Give the ring structure of $Q(\sqrt{-1}) \otimes_Q C$ in terms of simple rings.

ALGEBRA PRELIM

Fall 1976

The exam is in four parts. Justify all your answers.

I. Do 1 out of 2

II. Do 2 out of 3

III. Do 2 out of 3

IV. Do 2 out of 3

I. Linear Algebra

1. V a finite-dimensional vector space over a field k. Let $f \in \mathrm{End}_k(V)$.

   (i) Show that $V_1 = \bigcap_{n=1}^{\infty} f^n(V)$ and $V_2 = \bigcup_{n=1}^{\infty} \ker(f^n)$ are subspaces of V invariant under f, with $V = V_1 \oplus V_2$.

   (ii) Show that $f|V_1$ is an automorphism and $f|V_2$ is nilpotent.

2. Consider a form $ax^2 + bxy + cy^2$, where the coefficients are integers, and the variables x,y are to be given integer values. The discriminant of the form is the number $\Delta = b^2 - 4ac$.

   (i) If $\Delta < 0$, show that the form is positive or negative definite as $a > 0$ or $a < 0$.

   (ii) The form $ax^2 + bxy + cy^2$ is said to be equivalent to the form $AX^2 + BXY + CY^2$ if the first is carried to the second by a unimodular substitution, i.e.

$$x = pX + qY$$
$$y = rX + sY$$

   where p,q,r,s are integers with $ps - qr = 1$.
   Show that two equivalent forms have the same discriminant. Also show that the forms $X^2 + 6Y^2$ and $2X^2 + 3Y^2$ are inequivalent.

   (iii) A number n is said to be properly represented by the form if

$$n = ax^2 + bxy + cy^2$$

   for some relatively prime pair (x,y). Show that n is properly represented by a form $ax^2 + bxy + cy^2 \Longleftrightarrow$ there is an equivalent form $AX^2 + BXY + CY^2$, with $A = n$.

II. Group Theory

1. Let G be a finite group and $H \subset G$ a subgroup. Suppose that $G = \bigcup_{g \in G} g^{-1} Hg$. Show that if a prime number p divides the order of G, then p also divides the order of H.

2. Classify all isomorphism classes of groups of order 55.

3. Construct a non-abelian group of order 44 by means of the semi-direct product. Give a complete and explicit description of the group.

III. Fields, Rings, Modules

1. Let k be a field, and R a finite-dimensional commutative k-algebra with no non-zero nilpotent elements. Show that R is the direct product of fields.

2. Let S be a set, k a field and R a subring of the ring k^S of all functions from S to k where the multiplication on this ring is defined (pointwise) as

$$(f \cdot g)(s) = f(s) \cdot g(s).$$

a) Let T be a k-algebra. Show that $R \otimes_k T$ can also be viewed as a ring of functions from S to T under pointwise multiplication.

b) Show that if R and T are integral domains, then so is $R \otimes_k T$.

3. Let R be any ring, and let T be a non-split extension of a simple R-module M by a simple R-module N:

$$0 \to N \to T \to M \to 0.$$

Suppose that $N \not\cong M$. Show that every non-zero R-endomorphism of T is an isomorphism.

IV. Fields and Galois Theory

1. Let k be a field of characteristic $p \neq 0$, and let $\bar{k}$ be an algebraic closure of k. Define

$$k(1/p^{\infty}) = \{a \in \bar{k} \mid \exists n \text{ with } a^{p^n} \in k\}$$

Show that $k(1/p^{\infty})$ is a perfect field.

2. Let k be a field, $\bar{k}$ an algebraic closure. Let $k \subset L$, $T \subset \bar{k}$ be two intermediate fields. Let M be the subfield of $\bar{k}$ generated by L and T.

(i) Show that if L and T are finite Galois extensions of k, so is M.

(ii) Suppose that one of the following two (equivalent) conditions holds on L and T

(*) L and T are linearly disjoint over k, i.e. $L \otimes_k T \xrightarrow{\text{mult}} \bar{k}$ is an injection.

(**) $\dim_k M = \dim_k L \cdot \dim_k T$ Show that

$$\text{Gal}\,(M/k) \cong \text{Gal}\,(L/k) \oplus \text{Gal}\,(T/k).$$

3. Give examples of Galois field extensions K of the rationals Q, where

(i) Gal (K/Q) = symmetric group on 3 letters.

(ii) Gal (K/Q) = cyclic group of order 6.

ALGEBRA PRELIM SPRING 1976

Directions

1. The exam is in five parts. In part I you should answer as many questions as you can, but at least 4 of them. Be sure to allow plenty of time for the other four parts.
2. In parts II-V, where you have a choice of problems, mark clearly the problems you wish to have graded. Two half problems do not equal one problem.
3. You should write enough so that there is no doubt as to whether or not you know what's going on. In particular, if you use a big standard theorem, explain why it is applicable. (Do not feel obliged to state it in detail.) But use common sense. Don't write a book when a few lines are sufficient. When in doubt, ask.
4. Neatness counts in that illegible or very difficult-to-read exams will not be graded.

Part I State whether each of the following statements is true or false. If the statement is true give a short proof. If it is false, give a counterexample or otherwise disprove it.

1. There exists an Artinian integral domain which is not a field.
2. If N is a normal subgroup of a group G and $N \cap G' = \langle e \rangle$, where G' is the commutator subgroup and e the identity element of G, then N is contained in the center of G.
3. The Galois group of $x^3 + 3x^2 + 3x + 2$ over the field Q of rational numbers is Z_2.
4. If R is a Dedekind domain, then so is the polynomial ring $R[x]$.
5. There exist 11-dimensional subspaces U and V of a 20-dimensional vector space W such that $U \cap V = 0$.
6. Let C be the field of complex numbers. If $f \in C[x_1, \ldots, x_n]$ and $V = \{p \in C^n \mid f(p) = 0\}$, then f is irreducible if and only if V is irreducible.
7. A field F is an algebraic closure of a field K if and only if F is algebraic over K and for every algebraic extension E of K there is a K-monomorphism $E \to F$.

Part II Answer one of the following questions.

8. Let A and B be idempotent matrices over a field (that is $A^2 = A$ and $B^2 = B$). Prove: A and B are similar if and only if A and B have the same rank.

9. Let K be the field $Z_2(y)$ of all rational functions of y over the field of two elements. Find the Galois group over K of the polynomial

$$f(x) = (x^2 + y)(x^2 + yx + y) \in K[x].$$

Justify your answer.

10. Describe the structure of all rings R which have no nilpotent elements and satisfy the descending chain condition on left ideals.

Part III Answer one of the following questions.

11. If H is a subgroup of G with $H \neq G$ and $[G:H]$ finite, then there exists a subgroup N of H such that N is normal in G and $[G:N]$ is finite.

12. Let H be a proper normal subgroup of a finite group G. Suppose p is a prime which divides the order of H and T is a Sylow p-subgroup of H. Prove that

$$G = HN,$$

where N is the normalizer of T in G.

13. Prove or disprove: there is a simple group of order 48.

Part IV Answer one of the following questions.

14. A square matrix A over a field is diagonalizable if there exists a nonsingular matrix Q such that QAQ^{-1} is a diagonal matrix. Two square matrices A and B over a field are simultaneously diagonalizable if there exists a nonsingular matrix P such that both PAP^{-1} and PBP^{-1} are diagonal matrices.
Prove: If A and B are each diagonalizable and $AB = BA$, then A and B are simultaneously diagonalizable.

(continued on next page)

Part IV continued

15. Let K and F be fields with $K \subset F$. Let V be an n-dimensional vector space over K and $f: V \to V$ a K-linear transformation. Prove:
   (a) $F \otimes_K V$ is an n-dimensional vector space over F.
   (b) $1_F \otimes f: F \otimes_K V \to F \otimes_K V$ is an F-linear transformation.
   (c) The characteristic polynomial of $1_F \otimes f$ in $F[x]$ actually lies in $K[x]$ and is equal to the characteristic polynomial of f in $K[x]$.

Part V Answer two of the following questions.

16. Let G be the multiplicative group of units in the ring Z_{77}. Is G a cyclic group? What is the order of G? Justify your answers.

17. Find the Jacobson radical of the following rings.
   (a) The endomorphism ring of the abelian group $Z \oplus Z_2$.
   (b) $Q[x]/(x(x-1)^3)$, where Q = rational numbers.
   (c) The ring of $n \times n$ upper triangular matrices over a field (that is, matrices (a_{ij}) with $a_{ij} = 0$ for all $i > j$).

18. Let R be the field of real numbers. In $R[x,y]$, for what polynomials f is the ideal (f) a radical ideal? In terms of the prime factorization of f, how many irreducible components appear in a decomposition of the curve $f(x,y) = 0$?

19. If $K \subset E \subset F$ are fields with F Galois over K, then there exists a unique field L such that
   (i) $E \subset L \subset F$;
   (ii) L is Galois over K;
   (iii) if $E \subset M \subset F$ with M Galois over K, then $L \subset M$;
   (iv) the Galois group of F over L is

$$\bigcap_{\sigma \in G} \sigma H \sigma^{-1}$$

   where H is the Galois group of F over E and G is the Galois group of F over K.

(continued on next page)

Part V continued

20. Let R be a left Artinian ring with identity. Prove:

(a) If M is a maximal ideal of R, then M is the intersection of all maximal <u>left</u> ideals of R which contain M.

(b) If L is a maximal left ideal of R, then there exists a maximal ideal M with $M \subseteq L$.
[<u>Hint</u>: let M be the annihilator of R/L.]

(c) The Jacobson radical J of R is the intersection of all the maximal ideals of R.

(d) R has only finitely many maximal ideals.

ALGEBRA PRELIM FALL 1975

Directions:

The exam is in five parts. Part I is a true-false question. You should spend about 75 minutes on this part, which should enable you to do about 10 of the 15 questions. Don't try to do them all. In each of Parts II, III, IV and V you should do one (1) of the 2 or three questions. Indicate clearly which one you have done.

You should write enough so that there is no doubt about whether you know what is going on. But use common sense. Don't write a book. If you wish to use a major theorem, do so, and indicate why the theorem is applicable, but do not feel compelled to state the theorem in detail.

Neatness counts.

One complete solution is better than two partial solutions.

PART I. This is a "true-false" question. State whether each statement is true or false and give a short proof or disproof (a disproof would most often be a counterexample). You should probably spend about 75 minutes on this part, and should do 8 to 10 of the 15 parts.

1. There is no polynomial of degree 4 with integer coefficients whose Galois group over Q is cyclic of order 12.

2. If G is a group with a normal subgroup N such that $|G/N| = 3$ and N is cyclic of order 25, then G is Abelian.

3. Every (unitary) module over a ring with identity has a maximal proper submodule.

4. Let R be a semisimple ring with minimum condition and let ${}_R R = L_1 \oplus \ldots \oplus L_n$ be a decomposition of R as a direct sum of minimal left ideals. Then R is commutative if and only if $i \neq j$ implies $L_i \not\cong L_j$.

5. All 4x4 matrices T over R (the field of real numbers) satisfying $T^2 = -1$ are similar.

6. There is a field k and an integer n, $n > 0$, and a set S in k^n such that S is an intersection of hypersurfaces, but not the intersection of a finite number of hypersurfaces. (Definition: a hypersurface is a set of the form $\{\underline{x} : f(\underline{x}) = 0\}$, for some fixed polynomial f.

7. There exists an epimorphism of Abelian groups $f : Z_3 \oplus Z_2 \to Z_4$ whose kernel contains an element of order 4.

8. There is no Dedekind domain R such that for some ideal I in R, $R/I \cong Z_2[x,y]/(x^2,y^2,xy)$.

9. If F_0, F_5, and F_7 are the splitting fields of the polynomial x^3-2 over the fields Q, Z_5, and Z_7, then the degrees of these extension fields are all different.

10. If R is a commutative ring with 1 and $\phi: R^m \to R^n$ a surjective module homomorphism, then $m \geq n$.

11. If R is a commutative ring with identity such that every ideal except R itself is prime, then R is a field.

12. $x^3 - 9$ is irreducible in $Z_{31}[x]$.

13. For every quadratic extension K of a field k, there is an $\alpha \in k$ such that $K = k(\sqrt{\alpha})$.

14. For every nonconstant polynomial $g(x) \in Z[x]$, there are infinitely many primes p such that $g(x) \equiv 0 \pmod p$ has an integer solution.

15. If G is a group of order 216 then G has a normal subgroup N such that $8 \leq |N| \leq 60$.

<u>PART II.</u> Do one of the following 3 problems.

1. Prove that every prime ideal of $C[x,y,z]$ (where C is the ring of complex numbers) is an intersection of maximal ideals.

2. Construct explicitly (i.e. give the elements) a normal cubic extension K of Q such that $Q \subset K \subset Q(\xi)$, where ξ is a primitive 7th root of 1. (Hint: recall $Gal(Q(\xi)/Q \cong (Z/7Z)^*$.)

3. Let G be a subgroup of $GL(n,C)$ whose points are exactly those elements of $GL(n,C)$ which are the zeros of a certain family of polynomials. It is known that there is a unique irreducible component G_0 of G, in the Zariski topology, which contains the identity element of G. Prove

   (a) G_0 is a subgroup

   (b) G_0 is normal

   (c) G_0 has finite index in G.

PART III. Do one of the following problems

Let G be a finite group such that distinct subgroups have distinct orders. Prove that G is cyclic. (Hint: find an element of prime order and use induction.)

2. Give a complete classification for countable Abelian groups G such that $14G = 0$, (i.e. groups such that for all $x \in G$, $14x = 0$) (Hint: first try groups such that $2G = 0$.)

PART IV. Do one of the following problems

1. Let P be a finitely generated prime ideal of a commutative ring R with 1. Suppose $\mathrm{Ann}(P) = \{r \in R: rP = 0\} = 0$. Prove that $\mathrm{Ann}(P/P^2) = P$. (Hint: for any $n \times n$ matrix A, over a commutative ring, there is a matrix A^* such that $A^*A = (\det A)\, 1_n$. (A^* is the matrix of cofactors.).)

2. Let V and W be finite dimensional vector spaces over a field k. Say that two elements f and g of $\mathrm{Hom}(V,W)$ are <u>isomorphic</u> if there are automorphisms α and β of V and W such that $f = \beta g \alpha$ (linear transformations act on the left). Say that f and g are <u>V-isomorphic</u> if there is an automorphism α of V such that $f = g\alpha$.

   (i) how many isomorphism classes are there? Is it finite or infinite, or does this depend on k?

   (ii) same question for V-isomorphism classes.

PART V. Do one problem

1. Let R be a commutative ring and I an ideal of R. Note that any R/I module can be regarded as an R-module, and if M is any R-module, and $M[I] = \{x \in M: rx = 0 \text{ for all } r \in I\}$ then $M[I]$ can be regarded as an R/I module.
   Say whether each of the following statements is true or false, and give a proof or counterexample.

   (i) If M is an injective R/I module, then M is injective as an R-module.

   (ii) If M is an injective R-module, then $M[I]$ is injective as an R/I module.

PART V continued

Let θ be any root of x^3-2, $K = Q(\xi, \sqrt[3]{2}, \sqrt{7})$, where ξ is a primitive cube root of 1. Prove that $K \otimes_Q Q(\theta)$ is isomorphic as a ring to the direct sum of three copies of K. (Hint: the map $Q[x] \to Q(\theta)$ taking x to θ fits into an exact sequence.)

3. (a) Let R be a commutative ring with identity. Prove that the sum of a nilpotent element and a unit of R is a unit of R.

(b) Let $S = R[x]$, the polynomial ring over a commutative ring R with identity. Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in S$.
Prove that f is a unit of S iff a_0 is a unit of R and the a_i $(1 < i \leq n)$ are nilpotent. (Hint: If $b_0 + \ldots + b_mx^m$ is the inverse, show $a_n^{r+1}b_{m-r} = 0$, for all r.)

ALGEBRA PRELIM

Spring 1975

Directions

1. This exam is divided into four parts (A. Linear Algebra; B. Groups; C. Rings and Modules; D. Fields and Galois Theory).

   Do two problems in each part, a total of eight problems.

2. Mark clearly which eight problems you wish to have graded. Two half problems do not equal one problem.

3. You should write enough so that there is no doubt as to whether or not you know what's going on. In particular, if you use a big standard theorem, explain why it is applicable. (Do not feel obliged to state it in detail.) But use common sense. Don't write a book when a few lines are sufficient. When in doubt, ask.

4. Neatness counts in that illegible or very difficult-to-read exams will not be graded.

A. LINEAR ALGEBRA

1. A linear transformation T on a finite dimensional vector space V is said to be semi-simple if and only if $V = \oplus \sum_{i=1}^{n} V_i$ where for each V_i

   (a) $T(V_i) \subseteq V_i$

   (b) V_i contains no proper subspace W such that $T(W) \subseteq W$.

   Prove: A linear transformation T on a finite dimensional vector space V over a field is semi-simple if and only if the minimal polynomial of T is the product of distinct irreducible polynomials.

2. (a) Suppose T is a linear transformation on a finite dimensional vector space V over a field such that the minimal polynomial of T factors completely into distinct linear factors. Show that there is a diagonal matrix representing T.

   (b) Give an example of a linear transformation S on a vector space V over a field such that there is a diagonal matrix representing S, but the minimal polynomial of S factors into linear factors with a factor being repeated.

   (c) Give an example of a linear transformation P on a vector space V over a field such that the minimal polynomial does not factor into linear factors.

3. (a) Let V be a finite dimensional vector space over a field F, and suppose $V = X \oplus Y$ (for subspaces X and Y). Show that there is a <u>unique</u> linear transformation T on V such that $T|X = 1$ and $T(Y) = 0$. Such a map is called a <u>projection on X</u>.

   (b) Let V be a 2 dimensional vector space over the field R of real numbers (so that $V \cong R \oplus R$). Let X be the subspace spanned by $(1,-1)$. Give the matrices of <u>two distinct</u> projections on X.

   (c) Suppose $V = X_1 \oplus Y_1 = X_2 \oplus Y_2$ and T_i is the projection on X_i. Show that $X_1 \subseteq X_2$ if and only if $T_2T_1 = T_1$.

4. Let V be a fininte dimensional vector space over a field F and let

$$V^* = \mathrm{Hom}(V,F)$$

For a linear transformation $T:V \to V$, define $T^* \in \mathrm{End}_F(V^*)$ by

$$T^*(f)(v) = f(T(v))$$

or, more picturesquely,

$$(v, T^*(f)) = (T(v), f)$$

Show that

(a) T^* is 1-1 if and only if T is onto

(b) T^* is onto if and only if T is 1-1.

B. GROUPS

5. Prove or disprove each of the following statements.

   (a) If H is a subgroup of a finitely generated abelian group G and G is the internal direct sum of subgroups $G_1, \ldots, G_n$ (that is, $G = \oplus_{i=1}^{n} G_i$), then H is the internal direct sum of subgroups $H_1, H_2, \ldots, H_n$ $(H = \oplus \sum_{i=1}^{n} H_i)$, where each H_i is a subgroup of G_i.

   (b) If G is an abelian group and there is a monomorphism $\alpha : G \to G \times G$, then

$$\frac{G \times G}{\mathrm{Im}\ \alpha} \cong G.$$

50

6. (a) Exhibit a non-abelian group G with subgroups A and B such that
   (i) G is generated by A and B;
   (ii) A is normal in G;
   (iii) $A \cap B = \langle e \rangle$;
   (iv) A and B are abelian.

   (b) Show that for such a group G, there are homomorphisms

$$\begin{tikzcd} A \arrow[r, "\alpha"] & G \arrow[r, shift left, "\beta"] & B \arrow[l, shift left, "\gamma"] \end{tikzcd}$$

   such that

$$\alpha \text{ is a monomorphism}$$
$$\beta \text{ is an epimorphism}$$
$$\beta\gamma = 1_B$$
$$\operatorname{Ker} \beta = \operatorname{Im} \alpha.$$

7. Let H be a subgroup of a finite p-group G. Let C(H) be the set of cosets Ha of H in G.
   (a) Show that right translation defines an action of H on C(H)
   (b) Show that an element Ha in C(H) is a fixed point of this action if and only if $a^{-1}Ha = H$
   (c) Use (b) and a counting argument to deduce that there is an element $x \in G$ such that $x \notin H$ and $x^{-1}Hx = H$.

8. Suppose G is a group with a subgroup H of order 25 having 22 conjugates (including itself). Suppose the index of H in its normalizer in G is 11.
   (a) What must be the order of G?
   (b) Why <u>can't</u> the above situation occur?

C. RINGS AND MODULES

Note: all modules over rings with identity are assumed to be unitary (that is, $1a = a$ for all a).

9. Suppose R is a ring with identity such that every left R-module is the direct sum of simple sub-modules. Suppose M is a left R-module. Show that there is a finite set of left ideals $L_1, L_2, \ldots, L_k$ in R such that

$$M \cong \oplus\Sigma_{J_1} L_1 \oplus \oplus\Sigma_{J_2} L_2 \oplus \cdots \oplus \oplus\Sigma_{J_k} L_k$$ where $\oplus\Sigma_{J_i} L_i$ is the sum of J_i copies of L_i.

10. (a) Suppose R is a principal ideal domain with no cyclic injective modules. Show that no injective left module over R has finitely many generators.
    (b) Give an example of a ring S and an S-module M such that M is projective but not free.

11. (a) Let I be an ideal in a commutative ring R with identity. Show that

    $\{x \mid x^n \in I \text{ for some } n\}$ = the intersection of all prime ideals containing I.

    (b) Denoting the set given in (a) by $\sqrt{I}$, describe in detail the set of ideals I in the ring C[x] such that $I = \sqrt{I}$.
    (C[x] is the ring of polynomials over the complex numbers).

12. What is the Jacobson radical of each of the following rings?
    (a) The ring of formal power series with coefficients in a field K.
    (b) The polynomial ring K[x]
    (c) $K[x]/(x^7)$

    (d) The ring T_5 of all those 5×5 matrices with entries in K which have zeroes in every entry <u>above</u> the main diagonal.

13. Prove or disprove: Let R be a ring with identity which is left Noetherian (that is, the ACC on left ideals holds). Then every direct sum of injective left R-modules is injective.

D. FIELDS AND GALOIS THEORY

14. Let F be the field obtained by adjoining $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5}$ to the field Q of rational numbers Determine the Galois group of F over Q.

15. A Fundamental Theorem of Galois theory states that if a field K is separable over a field F and a splitting field for a polynomial in F[x], then the Galois Group of K over F has order [K:F].

    (a) Exhibit a non-separable field extension where the Galois group has only one element.

    (b) Exhibit a nontrivial separable field extension where the Galois group has only one element.

16. Consider $x^6 - 7$ as a polynomial over the field Q of rational numbers.

    (a) Show that $x^6 - 7$ is irreducible in Q[x].

    (b) Compute the dimension of the splitting field of $x^6 - 7$ over Q.

    (c) Determine the Galois group of $x^6 - 7$.

ALGEBRA PRELIM

Fall 1974

Directions:

1. This exam is divided into four parts (A. Groups; B. Rings and Modules; C. Fields and Galois Theory; D. Linear Algebra).

   Do a total of seven problems, including at least two problems in part A, two problems in part B, one problem in part C, and one problem in part D.

2. Mark clearly which seven problems you wish to have graded. Two half problems do not equal one problem.

3. You should write enough so that there is no doubt as to whether or not you know what's going on. In particular, if you use a big standard theorem, explain why it is applicable. (Do not feel obliged to state it in detail.) But use common sense. Don't write a book when a few lines are sufficient. When in doubt, ask.

4. Neatness counts in that illegible or very difficult-to-read exams will not be graded.

A. Groups

1. Find (up to isomorphism) all subgroups of order 8 of S_7.

   [Hint: You might want to notice that for each $n < 7$, you can consider S_n as the subgroup of S_7 which fixes all j with $n < j \leq 7$. Observe that if G is a subgroup of S_5, then there is a subgroup H of S_7 such that $|H| = 2$ and GH is the direct product of G and H.]

2. Let G be the group of all permutations of the set of positive integers. For each n identify the symmetric group S_n with the permutations of G which fix all $j > n$.

   Let A_n be the alternating group of degree n and let $A_\omega = \bigcup_n A_n$. Clearly A_ω is a subgroup of G.

   (a) Show that A_ω is simple. [Quote suitable theorems; no long proof needed.]

   (b) Show that A_ω has no nontrivial subgroups of finite index.

3. Prove that a group of order 48 has a normal subgroup of order 8 or 16.

A. Groups (continued)

4. Let V be finite-dimensional vector space over a field K and let G be a group of linear automorphisms of V. A subspace W of V is G-stable if $g(W) \subseteq W$ for all $g \in G$. V is G-semi-simple if, for every G-stable subspace W of V there is a G-stable subspace W' with $V = W \oplus W'$. Finally a G-stable subspace W is G-simple if it does not properly contain a G-stable subspace of V, other than (0).

   Suppose V is G-semi-simple and that H is a normal subgroup of G.

   a) Show that V is the sum of H-stable subspaces which are H-simple.

   b) Show that V is H-semi-simple.

B. Rings and Modules

5. If A is a minimal right ideal of a ring R (with or without 1) and $A^2 \neq 0$, then prove there is an idempotent $e \in A$ with $A = eR$.

6. Let R be a commutative ring and $a \in R$.

   a) Show that the set S of all ideals in R not containing any power of a contains a maximal element (with respect to set theoretic inclusion).

   b) Show that a maximal element in S is a prime ideal.

7. Let M be a free Z-module of rank n and f an endomorphism of M. Relative to any basis of M f is represented by an nxn matrix with integer entries. The determinant of f is by definition the determinant of any matrix representing f and is denoted det f.

   (a) Show that f is an automorphism if and only if $\det f = \pm 1$

   (b) Show that $M/f(M)$ is a finite abelian group if and only if $\det f \neq 0$.

   (c) Show that the order of $M/f(M)$ is precisely $|\det f|$ if $\det f \neq 0$.

B. Rings and Modules (continued)

8. (a) Let R be a ring and I,J left ideals of R, which are isomorphic (as R-modules). If $\phi: R \to R$ is a ring automorphism, show that $\phi(I)$ and $\phi(J)$ are isomorphic as R-modules.

(b) Assume that $L_1, L_2, \ldots, L_s$ are simple left ideals of R such that every simple left ideal of R is isomorphic (as an R-module) to one and only one of $L_1, L_2, \ldots L_s$. (In particular $L_i \cong L_j$ iff $i = j$).

For each i, let R_i be the sum of all left ideals of R which are isomorphic (as R-modules) to L_i.

If $\phi: R \to R$ is a ring isomorphism, then <u>prove</u> that ϕ permutes the set $\{R_1, R_2, \ldots, R_s\}$.

C. Fields and Galois Theory

9. Show that the Galois group over the field Q of rational numbers of $x^n - 1$ is isomorphic to the group of invertible elements in the ring Z/nZ.

[You may assume that the n-th cyclotomic polynomial $g_n(x)$ is irreducible in $Q[x]$; you will recall that $g_n(x) = \Pi(x-\zeta_i)$, where ζ_i ranges over all the primitive n-th roots of unity.]

10. Let K be a field, G a finite group of field automorphisms of K and let $F = \{a \in K \mid \sigma a = a \text{ for all } \sigma \in G\}$. F is clearly a subfield

(a) For $b \in K$, describe a non-zero polynomial $f \in F[x]$ such that $\deg f = |G|$ and $f(b) = 0$.

(b) For $b \in K$, find a non-zero <u>separable</u> $f \in F[x]$ with $f(b) = 0$.

(c) Using the above results and the existence of a primitive element for <u>finite</u> separable extensions, show that $[K:F] \leq |G|$. [Note: you must justify any claim that $[K:F]$ is finite.]

D. Linear Algebra

11. Let V be a finite dimensional vector space over a field K of characteristic different from 2. Let β be a bilinear form $V \times V \to K$, which is symmetric (i.e. $\beta(x,y) = \beta(y,x)$ for all x and y).

    (a) Show that if $\beta \neq 0$, there is a vector v such that $\beta(v,v) \neq 0$.

    (b) Use (a) to show that there is a basis for V such that the matrix of β is diagonal.

12. Let V be a finite dimensional vector space over a field F and for each $W \subset V$, let

$$A(W) = \{f \in \mathrm{Hom}_F(V,F) \mid f(W) = 0\}.$$

If W_1 and W_2 are subspaces of V, prove that

$$A(W_1 \cap W_2) = A(W_1) + A(W_2).$$

ALGEBRA PRELIM

Spring 1974

Directions:

1. This exam is divided into four parts (A. Linear Algebra; B. Groups; C. Rings and Modules; D. Fields and Galois Theory).

   Do two problems in each part, a total of eight problems.

2. Mark clearly which eight problems you wish to have graded. Two half problems do not equal one problem.

3. You should write enough so that there is no doubt as to whether or not you know what's going on. In particular, if you use a big standard theorem, explain why it is applicable. (Do not feel obliged to state it in detail.) But use common sense. Don't write a book when a few lines are sufficient. When in doubt, ask.

4. Neatness counts in that illegible or very difficult-to-read exams will not be graded.

A. LINEAR ALGEBRA

1. Let ϕ and ψ be endomorphisms of a finite dimensional vector space E (over a field). Assume that E has a basis of eigenvectors of ϕ and also a basis of eigenvectors of ψ. Assume that $\phi\psi = \psi\phi$. Prove that E has a basis consisting of vectors which are eigenvectors for both ϕ and ψ.

2. Let A and B be idempotent matrices over a field (i.e. $A^2 = A$, $B^2 = B$). Prove that A is similar to B if and only if A is equivalent to B. [Recall that A is equivalent to B means that there exist invertible matrices P,Q such that $B = PAQ$.]

3. Let V be a finite dimensional vector space over a field F and let W be a subspace of V. Let $A(W) = \{f \in \mathrm{Hom}_F(V,F) \mid f(w) = 0 \text{ for all } w \in W\}$. If W_1, W_2 are subspaces of V, prove that

$$A(W_1 \cap W_2) = A(W_1) + A(W_2).$$

B. GROUPS

4. If N is a normal subgroup of prime order p in the finite p-group G, then prove that N is contained in the center of G.

5. Determine up to isomorphism all groups of order 245 [i.e. exhibit (with proof) a list of groups of order 245, no two of which are isomorphic and such that every group of order 245 is isomorphic to some group on the list.]

6. (a) Prove that all automorphisms of S_3 are inner and that the group of all automorphisms of S_3 is actually isomorphic to S_3.

   (b) Construct an abelian group (of small order) whose automorphism group is isomorphic to S_3.

7. Prove that the additive group Q/Z (Q the rationals, Z the integers) is isomorphic to the group of all complex roots of unity.

C. RINGS AND MODULES

8. Determine all rings of order 2700 which are Jacobson semisimple. Give reasons for your answer.

9. Let R be a commutative ring with identity such that every submodule of every free R-module is free. Prove that R is a principal ideal domain.

10. Let $f(x) = \Sigma a_i x^i$ be a monic polynomial with coefficients in Z. For any $n > 1$, let $\bar{f}(x) = \Sigma \bar{a}_i x_i$, where $\bar{a}_i \varepsilon Z_n$ is the image of $a_i \varepsilon Z$ under the canonical map $Z \to Z_n$. Prove that if $\bar{f}(x)$ is irreducible over Z_n for some n, then f(x) is irreducible over the field of rational numbers.

11. Answer any 3 parts of this problem. True or false. If the statement is true, prove it. If it is false, give a counterexample (without proof).

   (a) If I is an ideal in a ring with identity such that every element of I is nilpotent, then I is a nilpotent ideal.

   (b) If M is a maximal ideal in a ring R with identity, then R/M is a field.

   (c) Every nonzero homomorphic image of a semisimple module A is semisimple.

   (d) Let F,A be unitary modules over a ring R with identity. If F is free and $F \otimes_R A = 0$, then $A = 0$.

D. FIELDS AND GALOIS THEORY

12. (a) If F is an extension field of dimension 2 over a field K, then prove that F is a normal extension of K.

    (b) If K is a finite field of characteristic p, prove that every element of K has a unique p-th root in K.

    (c) If K is a finite field then there is a homomorphism of rings from Z[x] onto K (where Z is the ring of integers).

13. Let F be a subfield of the complex numbers which is finite dimensional over the field Q of rationals. Assume [F:Q] is odd. Let p(x) be irreducible in Q[x] and assume all roots of p(x) lie in F. Prove that all the roots of p(x) are real.

14. Compute the Galois group of the following polynomials over the field Q of rational numbers

    (a) $x^5 - x^4 - 3x^3 + 3x^2 - 10x + 10$

    (b) $x^4 + x^2 + 1$

ALGEBRA PRELIM

AUTUMN 1973

There are 5 sections, entitled: Groups, Linear Algebra, Rings, Fields, Modules. Do 5 problems, one from each section. Indicate which 5 problems are to be graded.

Partial credit will be given. If you cannot do part of a problem, it is acceptable for you to use that part for later parts of the same problem.

If you use a standard big theorem, be sure to explain why it is applicable.

You should write enough so that there is no doubt that you know what is going on. But <u>use common sense</u>. Don't write a book when a few lines would suffice. When in doubt, <u>ask</u>.

GROUPS

1. Determine how many mutually non-isomorphic groups of order 12 there are, and describe each one. Include a proof that your list is complete. HINT: Think semidirect product.

2. A subset P of a group G is called a <u>positive cone</u> if (i) $1 \notin P$; (ii) if $x \neq 1$ then either $x \in P$ or $x^{-1} \in P$, but not both; and (iii) if x and y are in P, then $xy \in P$. The cone is <u>invariant</u> if for all $x \in G$, $xPx^{-1} = P$. If G is a group with a positive cone P, define $g < h$ to mean $hg^{-1} \in P$ and $g \leqslant h$ to mean $g^{-1}h \in P$.

   (a) Show that these two orderings on G coincide if and only if P is invariant.

   (b) Show that if G contains any non-identity element of finite order, then G contains no positive cone.

   (c) Show that if G is generated by two elements x and y of infinite order satisfying $xyx^{-1} = y^{-1}$, then G contains no invariant positive cone.

3. Let G be an abelian group in which every element has finite order. For each prime p, let $G_p = \{x \in G : p^n x = 0 \text{ for some integer } n \geq 0\}$. Prove that each G_p is a subgroup of G, and that G is the direct ~~product~~ sum of the subgroups G_p. Do not assume that G itself has finite order.

LINEAR ALGEBRA

1. Let V be a finite dimensional vector space over an algebraically closed field k, and let T and S be linear transformations from V to itself such that $ST = TS$.

   (a) If $\alpha \in k$ and $V_\alpha = \{x \in V \mid T(x) = \alpha x\}$, show that V_α is S-invariant.

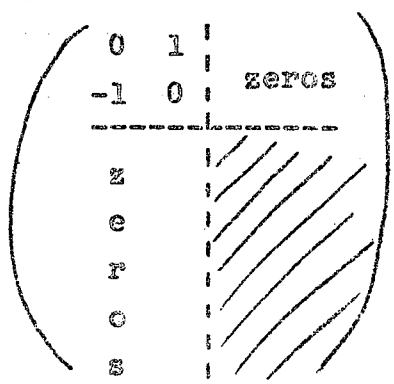
   (b) Show that S and T have a common eigenvector (with possibly different eigenvalues).

   (c) If G is a commutative group of linear transformations of V, show that V has a basis relative to which every element of G has a triangular matrix (i.e. a matrix with all entries below the main diagonal zero).

2. Let V be a finite dimensional vector space over a field k, and let $\beta: V \times V \to k$ be a bilinear form such that $\beta(x,x) = 0$ for all $x \in V$. (This implies that $\beta(x,y) = -\beta(y,x)$ for all $x,y \in V$.) Let $W = \{x \in V \mid \beta(x,y) = 0 \text{ for all } y \in V\}$.

   (a) If $x \notin W$, show there is some $y \in V$ with $\beta(x,y) = 1$.

   (b) Show there exists a basis for V relative to which the matrix of β has form:



assuming $W \neq V$.

   (c) Show that if β is non-degenerate, then V must be even dimensional.

3. Let V be a non-zero vector space. Prove that:

   (a) If S is any linearly independent subset of V, then there is a basis for V containing S.

   (b) If T is any subset of V which spans V, then some subset of T forms a basis for V.

   Do not assume V is finite dimensional.

RINGS

1. A Boolean ring is a ring R with more than one element such that $a^2 = a$ for all $a \in R$. You may assume every such ring is commutative. (Proof: expand $(a + a)^2$ and $(a + b)^2$.) Let R be a finite Boolean ring. Show that (a) R has an identity.
   (b) R has order 2^n for some integer $n \geq 1$.
   (c) R is characterized up to isomorphism by the integer n.

   HINT: Think Wedderburn.

2. Prove or give a counterexample (without proof):
   (a) Every unique factorization domain is a principal ideal domain.
   (b) Every unique factorization domain is Noetherian.
   (c) Every minimal prime ideal in a unique factorization domain is principal.
   (d) Every integral domain with 1 is a unique factorization domain.

3. Let R be a ring with 1.
   (a) If I is a nilpotent left ideal of R and $r \in R$, show that Ir is a nilpotent left ideal.
   (b) If I and J are nilpotent left ideals of R, show that $I + J$ is nilpotent.
   (c) The nil radical of R, N(R), is defined to be the union of all the nilpotent left ideals of R. Show that N(R) is a two-sided ideal.
   (d) If R is left Noetherian, show that N(R) is a nilpotent ideal.
   (e) Show by example that N(R) need not contain all nilpotent elements of R.

FIELDS

1. (a) Prove that a field with p^n elements (p a prime) is the splitting field over $F_p = Z/pZ$ of the polynomial $x^{p^n} - x$.

   (b) If K is the extension field of F_2 (the integers modulo 2) generated by a primitive 15th root of unity, z, (i.e. an element z such that $z^{15} = 1$ and $z^n \neq 1$ if $0 < n < 15$), is there an automorphism of K taking z to z^7? Justify your answer.

2. Let F be a field, F^* its algebraic closure, and K a subfield of F^* containing F, such that [K:F] is finite. We say K is a <u>normal</u> extension of F if it satisfies one of the following three equivalent conditions: (i) for every irreducible polynomial $f \in F[X]$, if K contains one root of f, it contains all roots of f (in F^*); (ii) every automorphism of F^* which fixes the elements of F, takes K into itself; (iii) K is the splitting field of a polynomial in F[X].

   The Fundamental Theorem of Galois theory states that if K is normal and separable over F, then the number of F-automorphisms of K is exactly the degree [K:F]. Show by example that this equality need not hold if the extension is

   (a) normal but not separable

   (b) separable but not normal.

   Prove your assertions.

3. Let F be the field of rationals and E the splitting field of the polynomial $x^4 + 2x^2 - 2$ over F.

   (a) What is the degree of E over F?

   (b) <u>Without</u> computing the Galois group, and <u>without</u> stating a great big theorem in detail, describe how information contained in the Galois group could be used to obtain information about subfields of E.

   (c) Compute the Galois group (as an abstract group)(but don't go back and give a lot of details in (b).)

MODULES

1. Let R be any ring, A be a right R-module, and B be a left R-module which is the direct sum of a family $\{B_i\}_{i \in I}$ of left R-modules. Prove that $A \otimes_R B$ is isomorphic to the direct sum of the family $\{A \otimes_R B_i\}_{i \in I}$.

2. Let R be any ring. An R-module Q is called <u>injective</u> if given any R-modules X, Y and any R-module map $f: Y \to Q$ and any injective (one-to-one) R-module map $g: Y \to X$, there is an R-module map $\phi: X \to Q$ such that $\phi g = f$.

$$\begin{tikzcd} & Q & \\ 0 \arrow[r] & Y \arrow[u, "f"] \arrow[r, "g"'] & X \arrow[ul, dashed, "\phi"'] \end{tikzcd}$$

   (a) Prove that if G is an abelian group which is an injective $\mathbb{Z}$-module, then G is <u>divisible</u>; i.e. given any $x \in G$ and any positive integer n, there is some $y \in G$ with $ny = x$.

   (b) Prove that if Q is an injective R-module and if $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is any exact sequence of R-modules, then the sequence $0 \to \mathrm{Hom}(C, Q) \to \mathrm{Hom}(B, Q) \to \mathrm{Hom}(A, Q) \to 0$ is also exact.

3. Let M be a left R-module satisfying the descending chain condition on submodules. Show that M has only a finite number of nonisomorphic, simple submodules. (i.e. there are a finite number of simple submodules such that any simple submodule is isomorphic to exactly one on this list.)

Algebra Prelim

SPRING 1973

Directions: Do your best to answer the required number of questions in each section. As a general rule it is better to answer fewer questions well rather than many questions partially or superficially.

Answer a total of 8 questions. Two of these must be in part I (Groups), two in part II (Fields and Galois Theory), and four in part III (Rings, Modules and Linear Algebra).

Part I. GROUPS

1. Show that every group of order 56 has a nontrivial normal subgroup. Do the same for groups of order 30.

2. (a) If p is the smallest prime dividing the order of a finite group G and H is a subgroup of index p in G, then prove that H is normal in G.

   (b) If G is a finite group which contains a subgroup of order n for each n dividing the order of G, then G is solvable.

3. Definition. A group is nilpotent if it is the direct product of its Sylow subgroups.

   Suppose that G is a finite group with the property that for each $g \neq 1$ in G,

$$C_G(g) = \{x \mid gx = xg\} \text{ is a nilpotent group.}$$

Let p,q be distinct primes and suppose that P is a p-Sylow subgroup of G and Q is a q-Sylow subgroup of G. Suppose that

$x \in P$ and $y \in Q$ are non-identity elements such that $xy = yx$.

(a) Prove that $xz = zx$ for every z in the center $Z(Q)$ of Q.

(b) Prove that x commutes with every element of Q.

(c) Prove that if $a \in P$ and $b \in Q$ then $ab = ba$.

4. We say that a non-trivial normal subgroup M of G is a <u>minimal normal</u> subgroup of G if

$$1 \subseteq N \subseteq M \text{ and } N \text{ normal in } G \text{ imply } N = 1 \text{ or } N = M.$$

Prove that if M is a minimal normal subgroup of a <u>solvable</u> group G, then M is an abelian p-group for some prime p.

Part II <u>FIELDS AND GALOIS THEORY</u>

5. Let F be a splitting field of the polynomial $x^5 - 5$ over the field Q of rational numbers. What is the dimension of F over Q? Why?

6. Suppose that $a_1, \ldots a_n$ are the roots of the polynomial $x^n - 1$ over the field Q of rational numbers. Assume that $a_1 + a_2 + \cdots + a_n$ is an integer. Prove that whenever k is relatively prime to n, then

$$a_1^k + a_2^k + \cdots + a_n^k = a_1 + a_2 + \cdots + a_n .$$

[<u>Hint</u>: you may assume that all primitive n-th roots of unity are roots of the same irreducible polynomial $g(x) \in Q[x]$.]

7. (a) <u>Prove</u> or <u>disprove</u>: If f(x) and g(x) belong to K[x] where K is a field, <u>and if the splitting fields of f(x) and g(x) over K are isomorphic</u>, then f(x) and g(x) have a non-trivial common factor.

(b) <u>Give examples</u>, <u>without proof</u>, of polynomials whose Galois groups are respectively the cyclic and the noncyclic group of order 6.

(c) Let F be an algebraic extension field of K and $u_1, \ldots, u_n \in F$. <u>State without proof</u> conditions which imply that there exists $u \in F$ such that $K(u_1, \ldots, u_n) = K(u)$.

(d) Let F be an extension field of K and let E be an intermediate field. Suppose σ is a homomorphism of E into F which fixes K elementwise. <u>State without proof</u> conditions which imply that σ can be extended to an automorphism of F.

Part III RINGS, MODULES AND LINEAR ALGEBRA

8. Definitions:

1. An element r of a ring R is nilpotent if $r^n = 0$ for some n.
2. $N(R)$ denotes the set of all nilpotent elements of R.

(a) If R is commutative, show that $N(R)$ is an ideal.

(b) If R is commutative, then

$$N(R/N(R)) = 0.$$

(c) Give an example of a noncommutative ring R such that $N(R)$ is not an ideal.

9. (a) Let R be a ring with identity and I the set of all elements in R which do not have multiplicative inverses.
Suppose that I is an ideal. Characterize R/I.

(b) Suppose that R is a commutative ring with identity such that for each $r \in R$ either r or $1-r$ has a multiplicative inverse. Prove that if J is the Jacobson radical of R, then R/J is a field

10. Suppose that A,B are $n \times n$ matrices with entries in a field F. Prove that $A^{-1}BA$ and B have the same characteristic polynomial and the same trace.

11. Suppose R is a ring without zero divisors which has a field F in its center. Prove that if the vector space dimension of R over F is finite then R is a division ring.

12. (a) Suppose L is a minimal left ideal in a ring R. Show: Either $xy = 0$ for all $x,y \in L$ or L contains a nonzero idempotent e (i.e. $e^2 = e$).

(b) Suppose $e \in R$ is idempotent and R has an identity. Show that $R = I \oplus J$ where I and J are nontrivial left ideals.

(c) Give an example of a commutative ring R, not a field, that has no minimal left ideal.

13. Let A be a module which is generated by a family of simple submodules. Prove that A is a direct sum of simple submodules.

14. A ring R is said to be <u>reductive</u> if: For any left ideal I or R, R/I is a projective R-module.
Show that any finitely generated module M over a reductive ring R is projective.
[<u>Hint</u>: If M is generated by n elements consider M/K where K is generated by (n - 1) of them.]

ALGEBRA PRELIM FALL, 1972

Directions:

1. This exam is divided into four parts (A. Linear Algebra; B. Groups; C. Rings and Modules; D. Fields and Galois Theory). Do two problems in each part, a total of eight problems.

2. Mark clearly which eight problems you wish to have graded. Two half problems do not equal one problem.

3. You should write enough so that there is no doubt as to whether or not you do know what's going on. But use common sense. Don't write a book when a few lines are sufficient. When in doubt, ask.

4. Neatness counts in that illegible or very difficult-to-read exams will not be graded.

A. Linear Algebra

1. Let R be a commutative ring and let M and P be R-modules. Let $M^* = \mathrm{Hom}_R(M,R)$. If N is a submodule of M, let $A(N) = \{f \in M^* \mid f(x)=0$ for all $x \in N\}$.

   a) Let $\phi: M \to P$ be an R-module map. Define a map $\phi^t: P^* \to M^*$ by $(\phi^t(f))(x) = f(\phi(x))$ where $f \in P^*$ and $x \in M$. Prove that ϕ^t is an R-module map.

   b) With the notation of part a), prove that $\ker(\phi^t) = A(\mathrm{Im}(\phi))$.

   c) If R is a field and if dim M, dim P $< \infty$, prove that

   $$\dim \mathrm{Im}(\phi) = \dim \mathrm{Im}(\phi^t)$$

   and that

   $$\mathrm{Im}(\phi^t) = A(\ker \phi).$$

2. Let R be the field of real numbers and let V be the vector space of all polynomials $p \in R[x]$ such that $\deg p \leq 2$. Define $f_i \in V^* = \mathrm{Hom}_R(V,R)$, $i=1,2,3$, by

   $$f_1(p) = \int_0^1 p(x)\,dx$$

   $$f_2(p) = \int_0^2 p(x)\,dx$$

   $$f_3(p) = \int_0^{-1} p(x)\,dx$$

   Show that $\{f_1, f_2, f_3\}$ is a basis for V^*.

3. In each of the following either provide an example with the given properties or tell why no such example exists. In either case, justify your answer.

   a) A 3×3 matrix A such that $A \neq 0$, $A \neq I$ and $A^2 = A$.

   b) A linear transformation T on a three dimensional vector space V such that $T^4 = 0$, but $T^3 \neq 0$.

   c) A 3×3 matrix A such that A is singular but has no non-zero extries.

   d) A linear transformation T of a finite dimensional vector space V <u>onto</u> a finite dimensional vector space W such that T is not one-to-one.

   e) A 4×4 matrix whose minimal polynomial is of degree 5.

A linear transformation T on a 5-dimensional vector space V satisfies the equation $x^2(x-1)^3 = 0$

and no polynomial of smaller degree. Let

$$M = \{v \in V \mid (T-1)^3 (v) = 0\}.$$

a) Show that $T(M) \subseteq M$

b) Show that there is a subspace N of V such that

$$N \cap M = \{0\}$$
$$N + M = V$$
$$T(N) \subseteq N$$

c) If $v \in M$ then there is a polynomial $f(x)$ of minimal degree such that $vf(T) = 0$. Prove that this $f(x)$ must be a divisor of $(x-1)^3$.

B. Groups

1. Let Q be the rational numbers and let Z be the integers. For each prime p let

$$G_p = \{\frac{m}{p^n} \mid m,n \in Z\}.$$

Prove that $Q/Z \cong \bigoplus_p (G_p/Z)$.

2. Let p be a prime and let G be a group of order p^3. Prove that if G contains more than one normal subgroup of order p, then G is abelian and <u>not</u> cyclic.

3. a) State the Sylow theorems.

   Let G be a finite group and let S be a p-Sylow subgroup.

   b) Let N(S) denote the normalizer of S in G, i.e. $N = \{x \in G \mid x^{-1}Sx = S\}$. Prove that $N(S) = N(N(S))$.

   c) If H is a normal subgroup of G, then $H \cap S$ is a p-Sylow subgroup of H and HS/H is a p-Sylow subgroup of G/H.

4. a) Determine up to isomorphism all abelian groups A with the property: There is an infinite cyclic subgroup B of A such that the index of B in A is 6. State theorems to justify all assertions.

   b) Describe two abelian groups A and B such that

      (i) A and B are not cyclic

      (ii) A and B each have order 8

      (iii) A and B are not isomorphic.

      Prove explicitly (without using theorems) that A is not isomorphic to B.

5. Let G be a group of order 108.

   a) Cite a theorem which guarantees the existence of a subgroup H of G of order 27.

   b) Use a) to give a morphism of G into S_4 (the permutation group on 4 letters).

   c) Use b) to show that G has a <u>normal</u> subgroup of order 27 or 9.

C. Rings

1. Let R be a commutative ring with 1 and let R have exactly one maximal ideal M.
   a) Prove that $r \in M \iff 1-r$ is an invertible element of R.
   b) If N is a finitely generated R-module such that $N = M \cdot N$, prove that $N = 0$.

2. <u>Definition</u> The nil-radical of a ring R is the union of the nilpotent two-sided ideals of R. We denote it by N(R). Prove the following:
   a) If A, B, and C are rings with identity such that $A = B \times C$ (ring product) and I is an ideal of A, then there are ideals I_1 and I_2 of B and C respectively such that $I = I_1 \times I_2$
   b) If A, B and C are rings such that $A = B \times C$, then $N(A) = N(B) \times N(C)$
   c) Let R be the ring of all 4×4 matrices of the form

$$\begin{pmatrix} a & b & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & c & d \\ 0 & 0 & 0 & e \end{pmatrix}$$

   with a, b, c, d, e real numbers. Find the nil-radical N of R.
   d) Describe $\frac{R}{N(R)}$ where R is the ring in c).

3. Give examples of rings with the following properties. Justify your assertions about the rings by stating some theorems or well-known facts.
   a) R has no non-zero nilpotent left ideals but has non-zero nilpotent elements.
   b) R is an integral domain, but for any proper ideal I that is not maximal, R/I is not an integral domain.
   c) R has no proper two-sided ideals but has proper left ideals.
   d) R is artinian but is not Jacobson semi-simple.

4. Let M be a module with the property
   (π) Given a submodule X of M, there is a submodule Y of M such that $X + Y = M$ and $X \cap Y = (0)$.
   Suppose that K is a submodule of M. Show that <u>both</u> K and M/K have the property (π).

D. Fields and Galois Theory

a) State the Fundamental theorem of Galois theory.

b) Find the Galois group of $x^4 - 2$ over Q. Show some work here. Don't use a magic machine for producing Galois groups (e.g. Kaplansky's).

c) Illustrate the correspondences in the Fundamental theorem by finding the fixed field of each <u>normal</u> subgroup in the Galois group of $x^4 - 2$.

2. Suppse F is a field, $f(x) \in F[x]$ and $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\{\alpha_i\}$ are all of the roots of $f(x)$. Show that if $g(x)$ is any irreducible polynomial in $F[x]$ with a root in K, then g has all of its roots in K. <u>Note</u>: This should be proved directly. Please don't cite powerful theorems.

3. a) Consider $x^3 - 2$ as a polynomial over $Z/(5)$. <u>Construct</u> a finite field F that contains $Z/(5)$ and at least two roots of $x^3 - 2$. By "construct" we mean give a list of the elements in F and an algorithm for adding and multiplying the elements.

b) For any real number α, we will denote the smallest subfield of R (the reals) containing Q (the rationals) and α by $Q(\alpha)$. Either show that there is a Q isomorphism of $Q(e)$ onto $Q(\pi)$ or show that no such isomorphism can exist. (e and π are the usual real numbers denoted by these letters. You may use well-known algebraic facts about e and π.)

MAR 24 1972 25

Algebra Prelim

Spring 1972

1. This exam is divided into 5 parts:
   A. Groups, B. Linear Algebra, C. Fields, D. Rings, and E. Modules.
   Do a total of 6 problems including at least 1 from each part.

2. Indicate clearly which 6 problems you wish to have graded. 2 half problems do not equal one problem.

3. You are encouraged to cite theorems from the "common knowledge" of mathematics unless the problem calls upon you to prove such a theorem.

4. You should write enough so that there is no doubt as to whether or not you do know what's going on. But use common sense. Don't write a book when a few lines are sufficient. When in doubt, ask.

5. Neatness counts. Illegible exams are hard to read.

A Groups

1. a. Prove that a group of order 15 is cyclic.
   b. Prove that a group of order 30 has a normal subgroup whose order is either 3 or 5.
   c. Prove that a group of order 30 has an element of order 15.

2. If G is a group, Aut(G) denotes the group of automorphisms of G, I(G) denotes the group of inner automorphisms of G, and Z(G) denotes the center of G.
   a. Prove $I(G) \cong G/Z(G)$.
   b. Prove that I(G) is a normal subgroup of Aut(G).
   c. If H is a normal subgroup of G prove that there is a homomorphism $\varphi : G \to \mathrm{Aut}(H)/I(H)$ whose kernel is $H \cdot C_G(H)$, where

$$C_G(H) = \{g \in G : h = g^{-1}hg \text{ for all } h \in H\}.$$

B Linear Algebra

3. Let A be an nxn matrix over the field k. Let $\lambda_1, \ldots, \lambda_n$ be the characteristic roots of A (possibly repeated) in the algebraic closure of k. Let p(x) be a polynomial in k[x].

Prove that $p(\lambda_1), \ldots, p(\lambda_n)$ are the characteristic roots of p(A) in the algebraic closure of k.

Hint: You may have a use for triangular forms.

4. If V is a vector space over the field k, $V^* = \mathrm{Hom}_k(V,k)$ denotes the dual space of V. For $T : V \to W$ a linear transformation between <u>finite dimensional</u> vector spaces the dual transformation $T^*: W^* \to V^*$ is defined by

$$\left(T^*(f)\right)(v) = f\left(T(v)\right) \qquad f \in W^*,\ v \in V.$$

a. Prove that T is one to one if and only if T^* is onto.

b. Prove that T is onto if and only if T^* is one to one.

C Fields

5. Let k be the field of rational numbers. Let K be the splitting field of the polynomial x^n-1. Prove that the Galois group of K over k is abelian.

6. Give an example of each of the following. Justify each answer with a sentence or two.

   (a) An algebraic field extension which is an infinite extension.

   (b) An algebraic field extension which is normal but not separable.

   (c) An algebraic field extension which is separable but not normal.

   (d) An infinite field of characteristic $p \neq 0$.

   (e) A finite field with a non-prime number of elements.

   (f) A transcendental field extension.

7. A field K is called <u>algebraically closed</u> if every non-constant polynomial in K[x] has at least one root in K. Let K be algebraically closed and let $\sigma : F \to K$ be a homomorphism of fields. Let L be an algebraic extension of F. Prove that σ can be extended to a field homomorphism from L to K.

D Rings

8. Let R be a commutative domain with 1. An element $a \in R$ is said to be <u>irreducible</u> if for every factorization $a = bc$ in R, exactly one of b or c is invertable.

   a. State what it means for R to be <u>Noetherian</u>.

   b. Prove that if R is Noetherian every noninvertable element is divisible by an irreducible element.

   c. Prove that if R is Noetherian every noninvertable element is a finite product of irreducible elements.

9. Let R be a commutative domain with 1. R is said to be <u>strongly Euclidian</u> if there is a function d from $R-\{0\}$ to the positive integers satisfying:

   1) If $x,y \neq 0$ then $d(x) \leq d(xy)$.

   2) If $x,y \neq 0$ then $x = ty + r$ where $d(r) < d(y)$ or $r = 0$.

   3) If $x,y,\ x+y \neq 0$ then $d(x+y) \leq \mathrm{Max}\big(d(x),\ d(y)\big)$.

   Prove that a strongly Euclidian ring is either a field or isomorphic to the ring of polynomials in 1 variable over a field.

   <u>Remark</u> Without loss of generality it may be assumed that $d(1) = 0$ and $(\exists x)[d(x) > n] \rightarrow (\exists y)[d(y) = n+1]$.

10. Let k be a field and let A be an nxn matrix over k whose minimal polynomial factors into distinct irreducible polynomials. Let R be the ring of matrices of the form $p(A)$ where $p \in k[x]$ is a polynomial.

    a. Prove that R is commutative and has no nilpotent elements.

    b. Prove that R is isomorphic to a direct sum of fields.

E Modules

11. Let K be a field and let $R \subseteq K$ be a subring whose quotient field is K. Let M be an R module.

a. Give a K-vector space structure to $K \otimes_R M$.

b. If $M = N \oplus P$ (as R-modules) prove $K \otimes_R M = (K \otimes_R N) \oplus (K \otimes_R P)$

c. Let G be a finitely generated free abelian group. Prove that the number of summands in an expression of G as the direct sum of cyclic groups is uniquely determined.

12. If M is an R module let End(M) denote the endomorphism ring of M.

a. Prove that if M is a simple R module then End(M) is a division ring.

b. Prove that if M is indecomposable (not expressible as a nontrivial direct sum of submodules), then the only elements $a \in \mathrm{End}(M)$ satisfying $a^2 = a$ are 0 and 1.

c. Prove the converse to part b.

d. By considering the additive group of rational numbers, show that the converse to part a is false.

ALGEBRA PRELIM

FALL, 1971

Directions:

1. This exam is divided into four parts (A. Groups; B. Rings and Modules; C. Linear Algebra; D. Fields and Galois Theory). Do two problems in each part, a total of eight problems.

2. Mark clearly which eight problems you wish to have graded. Two half problems do not equal one problem

3. You should write enough so that there is no doubt as to whether or not you do know what's going on. But use common sense. Don't write a book when a few lines are sufficient. When in doubt, ask.

4. Neatness counts in that illegible or very difficult-to-read exams will not be graded.

A. Groups

1. (a) If H is a normal subgroup of order p (p prime) in a finite p-group G, then prove that H is contained in the center of G.

   (b) Show that (a) may be false if H is not normal in G.

2. If G is a group which is not cyclic of order two, then prove that G has a nonidentity automorphism. [Thoroughly justify any claim that a particular map is in fact an automorphism.]

3. (a) Define "solvable group".

   (b) Using your definition of solvable, prove that every subgroup and every homomorphic image of a solvable group G is solvable.

   (c) If N is a normal subgroup of a group G and N and G/N are solvable, then prove that G is solvable.

4. Let $\mathcal{B}$ be a family of normal subgroups of a group G and suppose that G is generated by the groups in $\mathcal{B}$. If N is a normal subgroup of G such that $N \cap B$ is the trivial (identity) subgroup for every B in $\mathcal{B}$, then prove that N is in the center of G.

B. Rings and Modules

5. Let R be a ring with identity

   (a) Define the terms "free R-module" and "projective R-module". [Your definition of projective should be in terms of maps and should not mention free modules.]

   (b) Prove that every free R-module is projective.

   (c) Give an example of a projective module which is not free. Justify your answer.

6. Let A be a finite dimensional algebra with identity over a field K

   (a) Show that A satisfies both the ascending and descending chain conditions on right and left ideals.

   (b) What can be said about the structure of A in each of the following cases:

      (i) A has no nonzero nilpotent ideals;

      (ii) A has no nonzero nilpotent elements;

      (iii) A has no zero divisors.

7. Let R be a commutative ring with identity and J an ideal of R which is contained in every maximal ideal of R.

   (a) For each $j \in J$, prove that $1_R - j$ is a unit in R.

   (b) If A is a cyclic R-module such that $JA = A$, then prove that $A = 0$.

8. A nonempty subset S of a commutative ring R with identity is said to be <u>multiplicative</u> if $0 \notin S$ and $a \in S$, $b \in S \Longrightarrow ab \in S$.

   If S is a multiplicative subset of R, prove that there is a prime ideal of R which is disjoint from S.

16

C. Linear Algebra

9. (a) If $\phi : E \to E$ is a linear transformation of a finite dimensional vector space E over a field K, then prove that there is a unique monic polynomial $f \in K[x]$ such that

   (i) $f(\phi) = 0$;

   (ii) $g \in K[x]$ and $g(\phi) = 0 \Rightarrow f$ divides g.

   (b) Give an example of a vector space E and linear transformation ϕ such that $K[x]/(f)$ is a field (where f is as in (a)). Give reasons for your answer.

10. (a) Prove that an $n \times n$ matrix A over a field K is similar to a diagonal matrix if and only if every elementary divisor of A is linear.

    (b) Classify under <u>similarity</u> all 5×5 nilpotent matrices A over a field K (i.e. state a finite list of matrices such that every nilpotent A is similar to exactly one matrix on the list). Justify your answers.

    (c) Which of the matrices on the list in (b) are <u>equivalent</u>? Justify your answer.

11. Let V and W be finite dimensional real inner product spaces and $f : V \to W$ a linear transformation. Prove that there is a unique linear transformation $f^* : W \to V$ such that

$$(f^*(w), v) = (w, f(v))$$

for all $v \in V$, $w \in W$ [where (a,b) denotes the inner product of a and b in either V or W as the case may be].

15

D. Fields and Galois Theory

12. Determine the Galois group of the polynomial $f = x^4 + x^2 - 6$ over the field Q of rational numbers. [Thoroughly justify any claim that a particular map is in fact an element of the Galois group of f.]

13. Let F be an algebraic extension field of a field K. Prove that the following conditions are equivalent.

    (i) For every algebraic extension field E of K there exists a K-monomorphism $E \longrightarrow F$.

    (ii) Every polynomial in $K[x]$ splits in $F[x]$.

    (iii) Every polynomial in $F[x]$ has a root in F.

    (iv) F has no proper algebraic extensions.

14. Let N be a finite-dimensional, normal separable extension field of a field K. Let G be the Galois group of N over K and let f be a polynomial in $K[x]$ which splits in $N[x]$ and has no multiple roots. Prove that f is irreducible if any only if G acts transitively on the roots of f in N (i.e. if u,v are roots of f, then there exists $\sigma \in G$ with $\sigma(u) = v$).

MAR 26 1971

Ph.D. preliminary examination in Algebra

Spring, 1971

Instructions: There are four parts to this examination: (1) Linear algebra, (2) Rings and modules, (3) Groups, (4) Fields. Do two problems from each section. Two half-problems does not equal one problem.

1. Linear algebra

1.1 Suppose that L is a linear transformation of a four dimensional vector space V to itself such that L satisfies $(x-2)^2 \cdot (x-3)^2 = 0$ and no polynomial of smaller degree. Show directly that V can be decomposed into the sum of two L-invariant subspaces of dimension two.

1.2 Suppose L is a linear transformation from a vector space V $\ni \dim V < \infty$ to a vector space W. Prove that there exists a linear transformation L' $\ni L' \neq 0$ from W to V such that $(L'L)(L'L) = L'L$.

Suppose A is a linear transformation from V to V such that $A^j \neq 0$ for $j < m$ but $A^m = 0$ where m is the dimension of V. Prove that the matrix for A relative to some basis of V is

$$\begin{pmatrix} 0 & & & & & & \\ 1 & 0 & & & & & \\ & 1 & 0 & & & & \\ & & 1 & 0 & & & \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & 0 & \\ & & & & & 1 & 0 \end{pmatrix}$$

MAR 26 1971 13

.4 (a) Let A be a linear transformation of a finite dimensional vector space over a field K. Prove that if the K-minimal polynomial for A has non-zero constant term, then A has an inverse which is a linear combination of powers of A

(b) Let D be an algebra with identity over a field K such that (i) $[D : K] = n < \infty$ and (ii) If a and b are non-zero elements in D, then $ab \neq 0$. Show that D is a division ring. Hint: To find an inverse for $d \in D$, look at its "minimal polynomial".

2. Rings and modules

2.1 A commutative ring is called Noetherian if every ideal is finitely generated. It satisfies the ascending chain condition if for every infinite ascending sequence of ideals, $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$, there is some n such that $I_n = I_{n+k}$ for all $k \geq 1$. Show that these properties are equivalent.

2.2 (a) Show that the additive group of the rationals is an injective Z-module. (Z is the ring of integers.)

(b) Describe all injective indecomposable Z-modules.

2.3 (a) Prove: If K is an algebraically closed field and D is a division ring containing K in its center such that $[D : K] = n < \infty$, then $D = K$.

(b) Give a complete description of all simple K-algebras A satisfying $[A : K] = r < \infty$ where K is algebraically closed.

2.4 Let R be a ring and I an ideal of R. For each of the following, either prove or give a counterexample.

(a) If R is an integral domain, then so is R/I.

(b) If R is semi-simple with minimum condition, then so is R/I.

(c) If R has A.C.C. on left ideals, then so does R/I.

(d) If R has a unique maximal left ideal, then so does R/I.

(e) If R has no simple left ideals, then so does R/I.

(f) If R is indecomposable (not the ring direct product of two two-sided ideals), then so is R/I.

3. Groups

3.1 (a) Show that the additive group of the rational numbers is not finitely generated.

(b) Show that a finite non-cyclic abelian group contains a subgroup isomorphic to $Z(p) \times Z(p)$, for some prime p (where $Z(p)$ is the group of integers modulo p). State carefully any theorems you use.

3.2 Let G be a group of order 48.

(a) Show that G has a subgroup of index 3.

(b) Find a set X with three elements and a non-trivial homomorphism of G into the set of permutations of X.

(c) Show that G has a normal subgroup of index 3 or 6.

3.3 Describe up to isomorphism all groups G satisfying both of the following properties:

(a) $|G| = 28$, (b) There exists an element g in G of order 4.

3.4 Suppose G is a finite group which is the direct product of its Sylow p-subgroups. Show that any subgroup H of G has the same property.

4. Fields

4.1 (a) Show that $f(x) = x^3-3x+3$ has exactly one real root and two complex roots.

(b) Describe the Galois group of $f(x)$ over the rationals, giving reasons for your description.

4.2 Let L be an algebraic extension of the field M and let F be an algebraic closure of L. An element u in L will be called <u>separable</u> over M if its minimal polynomial over M has no multiple roots in F. Using <u>this</u> definition of separable do the following:

(a) Show that u in L is separable if and only if the number of monomorphisms of $M(u)$ into F, leaving M pointwise fixed, is equal to $[M(u):M]$.

(b) Show that if u in L is separable over M, then every element in $M(u)$ is separable over M.

4.3 Let p be a prime number and F_p the field with p elements. <u>Construct</u> field extensions K and L of F_p such that

(i) $F_p \subseteq K \subseteq L$.

(ii) $K \neq L$.

(iii) K contains an element a such that the polynomial $x^p - a$ is irreducible over K.

(iv) $L = K(\beta)$ where β is a root of $x^p - a$.

Use basic definitions and justify all of your assertions and constructions.

4.4 An extension L of a field M is said to be <u>normal</u> if for some set S of polynomials over M, every polynomial in S splits over L and L is generated over M by roots of the polynomials in S.

Using <u>this</u> definition of "normal", show that if L is a normal extension of M and E is a field such that $M \subseteq E \subseteq L$, then E is a normal extension of M if and only if every automorphism of L that leaves ~~K~~ M pointwise fixed carries ~~M~~ E into itself.

Algebra Prelim - Fall 1970

The exam is divided into four parts, which can be described roughly as 1. linear algebra, 2. rings and ideals, 3. groups, 4. fields. The problems are numbered 1.1, 1.2, ..., 2.1,... Do at least one problem from each section, and at least six problems in all.

1.1. Let $\{a_{ij}\}$ $1 \leq i \leq n$, $1 \leq j \leq m$, be elements of a field k. Using the elementary theory of linear transformations of vector spaces, prove that the following two conditions are equivalent:
(i) $m \geq n$, and the number of independent solutions of the equations

$$\Sigma_{j=1}^{m} a_{ij}x_j = 0 \qquad (i = 1,\ldots,n)$$

is exactly $m - n$.
(ii) For any choice of elements b_i, $1 \leq i \leq n$, there is a solution of the set of equations

$$\Sigma_{j=1}^{m} a_{ij}x_j = b_i \quad (i = 1,\ldots,n).$$

1.2. Let V be a finite dimensional vector space over the field C of complex numbers, with an inner product (,). [That is, for any vectors x and y there is an element (x,y) of C, satisfying the rules $(x + z,y) = (x,y) + (z,y)$, $(rx,y) = r(x,y)$ for all $r \in C$, $(x,y) = \overline{(y,x)}$ (complex conjugate), and $(x,x) \geq 0$ for all x, with equality if and only if $x = 0$.] Let T be a linear transformation of V into itself satisfying the rule $(x,T(y)) = (T(x),y)$.

(a) Show that if W is a subspace of V such that $T(W) \subseteq W$, then $T(W^{\perp}) \subseteq W^{\perp}$, (where $W^{\perp}$ is the orthogonal complement of W).

(b) Use this to show that there exists an orthonormal basis

for V such that the matrix for T with respect to this basis is diagonal.

1.3. (a) Show that if k is a field and f a polynomial in k[X], there is a k-vector-space V and a linear transformation T of V into itself whose <u>minimal polynomial</u> is f.

(b) Describe (in terms of the rational canonical form) the similarity classes of 6×6 matrices over the field of real numbers, whose minimal polynomial is $x^4 + x^2$. How many similarity classes are there?

1.4. If A, B, and C are modules over a commutative ring R, show that there is a natural isomorphism

$$\mathrm{Hom}(A \otimes B, C) = \mathrm{Hom}(A, \mathrm{Hom}(B, C)).$$

If V is a finite dimensional vector space over a field k, and V* its dual space, the above formula specializes to

$$(V \otimes V)^* = \mathrm{Hom}(V, V^*).$$

Show that a bilinear form on V can be regarded as an element of $(V \otimes V)^*$, and that the bilinear form is nondegenerate if and only if the corresponding element of Hom(V,V*) is an isomorphism.

2.1. (a) Let A be a finite dimensional algebra with identity over a field k and suppose that A has no nilpotent ideals. Describe as fully as you can the structure of A.

(b) What simplifications occur if either (i) k is algebraically closed, or (ii) A has no zero divisors? Justify your answers in part (b) fully.

2.2. Let R be a commutative ring such that every ideal of R is finitely generated. Show that if M is a finitely generated R-module, then every submodule of M is finitely generated.

2.3. (a) Let k be an algebraically closed field. Define an irreducible algebraic variety in k^n.

(b) Let $f_1, \ldots, f_k$ be polynomials in n variables over k and let V be the set of elements $(a_1, \ldots, a_n)$ in k^n such that $f_i(a_1, \ldots, a_n) = 0$, $(1 \leq i \leq k)$. Let J be the ideal of $k[X_1, \ldots, X_n]$ generated by the elements f_i and let I be the set of all elements in $k[X_1, \ldots, X_n]$ which vanish on V. State carefully a theorem which describes the relation between the ideals I and J.

(c) Show carefully that if I is a prime ideal then V is an irreducible algebraic variety.

3.1. (a) Describe the isomorphism classes of Abelian groups of order 40, giving an example of one group in each class.

(b) What does it mean to say that a group is solvable?

(c) Show that every nontrivial finite p-group has a center containing more than one element.

3.2. Let G be a nonabelian group of order 20 which contains a cyclic subgroup of order 4. How many elements of order 10 does G contain? Explain your answer. (Hint: determine the number of elements of orders 1,2,4,5, and 20.) (Bonus: show that there is exactly one group, up to isomorphism, satisfying these conditions.)

4.1. (a) State carefully the fundamental theorem of Galois theory for a finite normal extension of a field of characteristic zero.

(b) Suppose K is a normal extension of F whose Galois group is S_3 (the symmetric group on three letters). How many distinct fields E are there satisfying $K \supseteq E \supseteq F$, and what are their degrees? How many of them are normal extensions of F and what are the degrees of the normal extensions?

4.2. Consider the polynomial $x^7 - 2$. What is the degree of the splitting field of this polynomial over the field of rational numbers? What is the order of the Galois group? Is it Abelian? Write down two automorphisms which, together, generate the Galois group.

4.3. Let K be a finite normal extension of a field F, let G be the Galois group of K over F, and N a normal subgroup of G. Let E be the fixed field of N. Show that if f is an irreducible polynomial over F and f has a root in E, then all roots of f are in E. (You may use the fact that if α and β are two roots of f in K, then there is a $g \in G$, such that $g(\alpha) = \beta$.)

4.4. Let α, β, and γ be the three roots (in the field of complex numbers) of the equation $x^3 - 2$. (a) Show carefully that the field $Q(\alpha)$ is not a normal extension of Q. (Q is the field of rational numbers.) (b) Show without computation that $(\alpha+1)(\beta+1)(\gamma+1)$ is rational. (You may use Galois theory.)

ALGEBRA PRELIM

SPRING 1970

Choose two problems from each section of the exam. If you should attempt more than two problems in a given section, be sure to mark clearly which two problems you wish to have corrected. Two halves of two problems does not equal one problem.

Linear Algebra

1.1 Let V be a vector space with a finite basis over a field F. Prove that any other basis for V over F is also finite and contains the same number of elements.

1.2 Let M be a module over a ring R and let $E(M) = \mathrm{Hom}_R(M,M)$ be the R-endomorphism ring of M. Let ε be an idempotent in $E(M)$, i.e. $\varepsilon^2 = \varepsilon$ and $\varepsilon \neq 0$. Prove that there are submodules M_1 and M_2 of M with $M = M_1 \oplus M_2$ and $\varepsilon(m_1 + m_2) = m_1$ for all $m_1 \in M_1$ and $m_2 \in M_2$.

1.3 Let V and W be finite dimensional vector spaces over a field F and let V^* and W^* be the dual spaces. Let $T : V \to W$ be an F-linear transformation and let $T^* : W^* \to V^*$ be the adjoint transformation. If bases for V and W are given, prove that the matrix of T^* relative to the dual bases is the transpose of the matrix of T relative to the given bases.

1.4 Let V be a finite dimensional vector space over a field K and let $T : V \to V$ be a K-linear transformation.

a) By considering polynomials in T, show that V is a $K[X]$ - module (X a 'variable').

b) Using the structure theorem for finitely generated modules over a principal ideal domain, describe the decomposition of V as a $K[X]$ - module.

c) Describe how this decomposition can be used to obtain the rational canonical form of the matrix of T.

Groups

2.1 Let S be a p-Sylow subgroup of a group G and let $N_G(S)$ denote the normalizer of S in G.

a) Show that $N_G(S) = N_G(N_G(S))$.

b) Let H be a normal subgroup of G. Prove that $H \cap S$ is a p-Sylow subgroup of H and that HS/H is a p-Sylow subgroup of G/H.

2.2 a) Prove that the number of elements in any conjugacy class of a finite group G divides the order of G.

b) Prove that the center of any finite p-group, p a prime, contains at least p elements.

c) Prove that any group of order p^2 is abelian.

2.3 If G is a group of order p^3, p a prime, and if G has more than one normal subgroup of order p, then G is abelian and not cyclic. Prove it.

2.4 a) Prove that a group of order 35 is abelian.

b) Find primes p and q such that there is a nonabelian group of order pq and construct this group.

Rings and Modules

3.1 a) State some form of the Wedderburn structure theorem for rings.

b) Let A be an algebra over a field k with $[A:k] < \infty$. Prove that A is isomorphic to a direct product of division algebras if and only if A has no nonzero nilpotent elements.

3.2 Let R be a ring such that $R^2 \neq \{0\}$ and the only right ideals of R are $\{0\}$ and R. Prove that R is a division ring. (Do not assume that R has an identity. Note that the following are all right ideals of R: $\{x \in R : xR = \{0\}\}$, aR, $\{x \in R : ax = 0\}$.)

3.3 Let R be a ring (with identity if you wish).

a) Define the nilradical N of R and the Jacobson radical J of R.

b) Show that $N = J$ if R satisfies the descending chain condition on left ideals (R is left Artinian).

c) Find an example where $N \neq J$.

3.4 Let R be a commutative ring with identity and let M, N, and P be R-modules. Let $M \otimes_R N$ denote the tensor product of M and N over R and let $\mathrm{Hom}_R(M,N)$ denote the R-module of R-homomorphisms from M to N

a) Prove that $\mathrm{Hom}_R(M \otimes_R N, P)$ is isomorphic as an R-module to $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P))$.

b) Find an example where $M \otimes_R N = \{0\}$ but neither M nor N are zero.

Fields and Galois Theory

4.1 State the Fundamental theorem of Galois theory and illustrate the correspondences with the splitting field of $X^3 - 2$ over Q, the field of rational numbers.

4.2 Let K be an extension field of a field F. If $x \in K$, let $F(x)$ be the subfield of K generated by F and x.

a) Prove that an element $x \in K$ is algebraic over F if and only if $F(x)$ is a finite extension of F.

b) Prove that the set of all elements of K which are algebraic over F forms a subfield of K.

4.3 Definition: A Galois extension K of a field k is the splitting field of a family of separable polynomials in $k[X]$.

Let K be a Galois extension of a field k and let G be the group of all k - automorphisms of K. Prove that

$k = K^G = \{x \in K : \sigma(x) = x \text{ for all } \sigma \in G\}$,

(Note that $[K:k]$ need <u>not</u> be finite.)

4.4 Let F be a finite field of characteristic p.

a) Prove that F has p^m elements for some integer m.

b) What is the structure of the additive group of F?

c) What is the structure of the multiplicative group of nonzero elements of F?

d) Describe the automorphisms of F.

5. (b) continued

(2) The ring of all continuous real valued functions on the unit interval

(3) $R(x)/(x^2+1)^5$ the real polynomial ring in x factored by the ideal generated by $(x^2+1)^5$.

6. Prove that <u>every</u> vector space over a field has a basis.

7. Show that if H is a subgroup of the finite group G then the order of H divides the order of G.