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 cubic 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 all 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 not 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 normal extension of $\mathbb{Q}$ of odd degree must be contained in $\mathbb{R}$.
   (b) Give an example of a normal 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).

   $\langle Ax,y\rangle = \langle A(x)^T, y =$

   (a) Show that $\langle Ax,y\rangle = \langle x,A^Ty\rangle$.

   (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.

96

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 $Gal(K/k)$ 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.

$V^* = \mathrm{Hom}_k(V, k)$

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 $G = H \times N$.

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.

9:30-12:30
Mon. March 22, 1982

ALGEBRA PRELIM

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.

3. 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 right 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 right 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 rigid motion 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 $\alpha \neq \beta$).

$$a)\ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix} \qquad b)\ \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$$

   (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 minimal 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 not 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 $f \in Q[X_1,\ldots,X_n]$, $(\sigma f)(X_i,\ldots,X_n) = f(X_{\sigma(1)},\ldots,X_{\sigma(n)})$ (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 $\mathrm{rank}(T_A) = n^2 - n$.

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

$$\mathrm{Ann}(A) = \{r \in R : ra = 0 \quad \text{for all} \quad a \in A\}.$$

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 briefly).

   $\mathbb{Z}$ $\qquad$ $\mathbb{C}[[X]]$ (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 simple 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 not 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 matrix 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 is 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 $g \in G$.