Algebra General Exam

January 1981

1. An 8×8 matrix has characteristic polynomial $x^2(x^4-1)(x^2-1)$.

   a) What are the possible Jordan forms for such a matrix over the complex numbers?

   b) If the matrix has entries from the real field, what are its possible canonical forms?

2. Let ζ be a primitive 7^{th} root of 1 over the rational field, $\mathbb{Q}$ (you may take $\zeta = e^{2\pi i/7}$).

   a) What is the minimal polynomial of ζ over $\mathbb{Q}$?

   b) What is the degree of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$?

   c) Determine the effect of any automorphism of $\mathbb{Q}(\zeta)$ on ζ and hence determine the Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$.

   d) What are the subfields of $\mathbb{Q}(\zeta)$?

3. It is claimed that a semi-simple algebra over the complex numbers, $\mathbb{C}$, has dimension 15 over $\mathbb{C}$, and has a center whose dimension over $\mathbb{C}$ is 3. Is this possible? (Give an argument supporting your conclusion.)

4. a) If k is a field, show that the polynomial ring k[x] is a Euclidean domain.

   b) Gauss knew that the polynomial ring, k[x,y], in two variables over the field k has unique factorization. Why is k[x,y] <u>not</u> a Euclidean domain?

5. A certain group of order 60 has precisely four elements of order 5; show that these elements together with the identity element form a normal subgroup.

Algebra General Exam

January 1982

I. If A is a 6×6 matrix with complex entries and characteristic polynomial $(x+2)^4(x-1)^2$ what are its possible Jordan cononical forms?

II. Let $f(x) = x^3 + 5x - 5$ over the field $\mathbb{Q}$ of rational numbers.

(a) Find the number of real zeros of $f(x)$.

(b) Show that $f(x)$ is irreducible over $\mathbb{Q}$.

(c) Determine the Galois group of $f(x)$.

(d) Is $f(x)$ solvable by radicals? (Give reasons for your answer).

III. Let A be a 5×5 matrix with complex entries, characteristic polynomial $(x-2)^3(x+7)^2$, and minimal polynomial $(x-2)^2(x+7)$.

(a) What is the trace of A?

(b) What is the determinant of A?

(c) What is the Jordan canonical form for A?

(d) Is A similar to a diagonal matrix?

IV. Let V be a two dimensional vector space over the real field and let (x,y) be a non-singular symmetric bilinear form on V with the property that there is a vector $v \neq 0$ in V with $(v,v) = 0$.

(a) Show that V has a basis e_1, e_2 with $(e_1,e_1) = 0$ and $(e_1,e_2) = 1$, $(e_2,e_2) = 0$

(b) Show that if α is any real number there is a vector u in V with $(u,u) = \alpha$.

V. Let A and B be two right modules over the commutative ring, R, which has 1.

(a) What is the tensor product $A \otimes_R B$?

(b) Show that $A \otimes_R R$ is isomorphic to A (as R modules).

(c) If $\mathbb{Z}_n$ is the group of integers modulo n, what is $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$?

VI. Let S be a multiplicative subset of the commutative, R, with 1 and let I be an ideal of R disjoint from S.

(a) Show that there is an ideal M of R with $I \subseteq M$, $S \cap M = \emptyset$ and maximal with respect to these properties.

(b) If $R = \mathbb{Z}$, the ring of integers, and $S = \{3^n : n \geq 0\}$ and $I = 2\mathbb{Z}$, what is M?

VII. a) Let G be a finite group, N a normal subgroup, and P a p-Sylow subgroup of N. Prove that $G = NN_G(P)$, where $N_G(P)$ is the normalizer of P in G.

b) The Frattmi subgroup F of G is the intersection of its maximal subgroups. Show that F is normal in G and use a) to show that each Sylow subgroup of F is also normal in G.

c) Find the Frattmi subgroup of S_4, the symmetric group on 4 letters; justify your answer.

September 14, 1982

ALGEBRA GENERAL EXAMINATION

1. Prove that if m is a positive integer, then $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} m\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$.

2. Let D be a principal ideal domain and let $a_1,\ldots,a_n$ be in D, not all 0. Let d be a greatest common divisor of $a_1,\ldots,a_n$ in D. Show that there is an invertible n by n matrix Q with entries in D for which

$$(a_1,\ldots,a_n)Q = (d,0,\ldots,0).$$

3. Describe the finite Abelian groups that have exactly three distinct composition series.

4. Prove that if F/K is an algebraic extension of fields, and every element of F belongs to an intermediate field between K and F that is normal over K, then F itself is normal over K.

5. Describe the Galois group of $x^4 + 2x^2 + 2$ over $\mathbb{Q}$. Determine the intermediate fields of the splitting field and display the Galois correspondance.

6. Prove that if G is a non-Abelian group of order 21, then G is generated by two elements s and t, s of order 7 and t of order 3, for which $t^{-1}st = s^2$.

7. A matrix A is called idempotent if $A^2 = A$. Prove that two idempotent n by n matrices with entries in a field are similar if and only if they are equivalent (associated).

8. Display two complex 4 by 4 matrices that have the same characteristic and minimal polynomials and yet are not similar.

9. Let R be a commutative ring with identity and let M be a maximal ideal. Show that if A is an ideal for which $M \supseteq A \supseteq M^k$ for some k, then A is M-primary.
From that, show that in $\mathbb{Q}[x,y]$, $(x^2, x+y)$ is a primary ideal not equal to a power of its radical.

Algebra Qualifying Examination March 26, 1983

1. Find the Jordan canonical form for the matrix $\begin{pmatrix} -1 & 3 & 0 \\ 0 & 2 & 0 \\ 2 & 1 & -1 \end{pmatrix}$ over the complex field.

2. Work out the Galois group of $\mathbb{Q}\left(\frac{1+\sqrt{2}}{1+\sqrt{3}}\right)$ over $\mathbb{Q}$.

3. Show that the symmetric group Sym_8 on eight letters contains a subgroup of order 15, but that Sym_n does not if $n<8$.

4. Prove that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to $\mathbb{Q}$.

5. Let D be a unique factorization domain in which the units, along with 0, form a proper subring. Show that D has infinitely many (nonassociate) primes. Give an example of such a domain.

6. Show that a finite Abelian group is cyclic if and only if it contains no subgroup isomorphic to a group of the form $A \times A$, other than the trivial subgroup consisting of the identity alone.

7. The finite field $GF(p^6)$ of p^6 elements is a Galois extension of $GF(p)$ (p is a prime). For x in $GF(p^6)$, the trace of x is the sum of the conjugates of x. Express the trace of x as a polynomial in x and then show that there is an x whose trace is nonzero.

8. Does 7 divide $10^{31} + 31^{10}$? Why?

Algebra general examination, Saturday, Sept. 10, 1983

Please show and explain your work. Even when you don't see your way through a problem, an outline of relevant methods and theorems may earn substantial credit.

1. Can there be a simple group of order 1776? How many isomorphism classes of Abelian groups of order 1776 are there? Is there a non-Abelian group of this order?

2. Prove that if a module has a composition series, it satisfies both chain conditions. Specify the theorems you invoke.

3. Prove that a finite multiplicative subgroup of a field must be cyclic. Give an example of a ring that is not a field, that contains a finite noncommutative multiplicative subgroup.

4. Assuming the polynomial $x^4 + ax^2 + 1$ to be separable and irreducible, find relationships among the roots and determine its Galois group. Explain from that why the coefficient field could not be finite.

5. If A is a 3 by 3 matrix with characteristic polynomial $x^3 + ax^2 + bx + c$, let $A^* = A^2 + aA + bI$. Show that if $\det A \neq 0$, then $A^* = (\det A)A^{-1}$, and $(A^*)^* = (\det A)A$. Why does this last formula continue to hold even when $\det A = 0$?

6. Find the Jordan canonical forms for the matrices

$$\begin{bmatrix} 0 & -1 & -1 & -1 \\ 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & -1 & 0 & -1 \\ 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{bmatrix}.$$

7. Let R and S be principal ideal domains with R a subring of S. Suppose a and b are in R and d is a greatest common divisor (gcd) of a and b in R. Show that d is also a gcd of a and b in S.

8. Let K be a finite dimensional Galois extension of $\mathbb{Q}$ and consider the bilinear form on K given by

$$\langle x, y \rangle = \mathrm{tr}(xy),$$

tr the trace from K to $\mathbb{Q}$. If σ is in the Galois group of K over $\mathbb{Q}$, determine the adjoint σ^* of σ relative to this form.

Mathematics: Algebra General Examination Feb 25, 1984

1. Describe the Abelian groups of order 1984. Describe at least two different non-Abelian groups of that order.

2. Determine the Galois group of x^3-2 over the rational field, $\mathbb{Q}$. Explain why the splitting of x^3-2 contains $\mathbb{Q}(\sqrt{-3})$.

3. If R is a finite commutative ring with identity, prove that every prime ideal must be maximal.

4. Write out the possible rational canonical forms over $\mathbb{Q}$ for the 6 by 6 matrices having minimal polynomial $(x-1)^2(x^2+1)$. For each one write out the corresponding Jordan normal form over $\mathbb{C}$, and list any further possible Jordan normal forms for that minimal polynomial not produced so far.

5. Factor x^3-y^3 into irreducible factors in $\mathbb{Q}[x,y]$ and prove that each really is irreducible.

6. Let F be a field and let θ be algebraic over F. Suppose the degree $[F(\theta):F]$ is odd. Prove that $F(\theta) = F(\theta^2)$.

7. Let H and K be subgroups of a group G. If $Ha = Kb$ for some a and b in G, show that $H = K$. What can one conclude from $aH = Kb$ instead?

8. If $\theta^5+\theta+1=0$, express $\frac{1}{\theta+1}$ (from $\mathbb{Q}(\theta)$) in terms of powers of θ.

Another File Copy

1985?

ALGEBRA TEST

Name: _____

Instructions: Put all your answers on the exam paper. Use the backs of the pages if necessary. Good luck!

1. **Group Theory.** (a) Does there exist a simple group of order 200? If there is such a group G, describe G explicitly. If no such G exists, explain, quoting carefully any theorems you are using in your explanation.

(b) Give a specific example of a finite, nonabelian simple group G. No proofs required!

(c) Up to isomorphism, how many finite abelian groups of order $2^3 \cdot 3^4$ are there? Give an example for each isomorphism class.

2. **Linear algebra.** Consider the (real) matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{bmatrix}.$$

(a) What is the characteristic polynomial f(x) of A?

(b) What is the minimum polynomial of A?

(c) What is the Jordan canonical form of A? (You need not find the matrix P such that PAP^{-1} is in Jordan form.)

3. Rings and Fields. (a) Prove that the polynomial $f(x) = x^5 - 6x^3 + 12x^2 + 21x - 3$ is irreducible over $Q[x]$.

(b) Let $F = F_7$ be the field having 7 elements. Fix an element $\xi \in F$, and consider the set K_ξ of all matrices of the form $\begin{bmatrix} a & b \\ \xi b & a \end{bmatrix}$, $a,b \in F$. Show that K_ξ is a subring of the ring $M_2(F)$ of all 2×2 matrices with coefficients in F. For what elements $\xi \in F$ is K_ξ a field (of order 49)?

(c) Suppose that a, b are relatively prime positive integers. Show that the ring Z_{ab} of integers mod ab is isomorphic to the direct product ring $Z_a \times Z_b$. Corollary: If a positive integer m is written as a product $p_1^{e_1} \cdots p_t^{e_t}$ for distinct primes $p_1, \cdots, p_t$, then Z_m is isomorphic to the direct product $Z_{p_1^{e_1}} \times \cdots \times Z_{p_t^{e_t}}$. Why (in ≤ 1 word)?

(d) Show that if R is a commutative ring, then $x + y$ is nilpotent whenever x and y are nilpotent elements in R. (An element x is nilpotent if $x^n = 0$ for some positive integer n.) Give an example of two nilpotent elements x,y in a noncommutative ring R such that $x + y$ is not nilpotent.

Algebra qualifying examination - Sept. 8, 1984 (pledged)

10 1. Prove that there is no simple group of order 72.

15 2. Let L be a left ideal in a ring R and put

$$I(L) = \{a \in R \mid La \subseteq L\}.$$

Prove that $I(L)$ is the largest subring S of R such that L is a two-sided ideal of S. Prove that R is a division ring if and only if $I(L) = L$ for all nonzero L.

15 3. Let E be a Galois extension of $\mathbb{Q}$ of degree 4. Prove that $E = \mathbb{Q}(\theta)$ where θ is a root of a polynomial of the form $x^4 + ax^2 + b$, $a, b \in \mathbb{Q}$. Show that the Galois group is cyclic if and only if b is not a square in $\mathbb{Q}$.

15 4. Let D be the linear transformation on the four dimensional real vector space spanned by the functions $x\sin x$, $x\cos x$, $\sin x$, and $\cos x$, given by differentiation. Find the characteristic and minimum polynomials, the invariant factors, and the rational canonical form of D. Find the Jordan normal form of D when complex coefficients are allowed.

$$\begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad \begin{matrix} 1, (\lambda^2+1)^2 \\ (\lambda^2+1)^2 \\ (\lambda^2+1)^2 (\lambda^2+T)^2 \end{matrix}$$

$$\begin{bmatrix} 0 & & -1 & \\ 1 & 0 & & 0 \\ & 1 & 0 & -2 \\ & & 1 & 0 \end{bmatrix}$$

10 5. Prove the modular law for submodules A, B, C of a module: if $A \supseteq C$, then $(A \cap B) + C = A \cap (B + C)$.

$$\begin{bmatrix} 1 & i & & \\ & & & \\ & -i & & \\ & 1 & -i & \end{bmatrix}$$

(or transp)

10 6. Find the invariant factors over $\mathbb{Z}$ of the matrices shown. Are they integrally equivalent? No

$$\begin{bmatrix} 2 & & \\ & 2 & \\ & & 60 \end{bmatrix} \quad \begin{bmatrix} 2 & & \\ & 4 & \\ & & 120 \end{bmatrix}$$

$$\begin{bmatrix} 10 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{bmatrix}, \quad \begin{bmatrix} 4 & 6 & 4 \\ 4 & 20 & 12 \\ 20 & 0 & 20 \end{bmatrix}$$

7. The polynomial $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$ will factor into irreducible factors in various ways when regarded as a member of $GF(q)[x]$, depending on q. Determine the possible factorings as a function of q. ($\sqrt{2} \in GF(q)$, otherwise ...)

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2 & 2 & \cdots & 2 \\ 1 & 2 & 3 & 3 & \cdots & 3 \\ 1 & 2 & 3 & 4 & \cdots & 4 \\ & & & \cdots & & \\ 1 & 2 & 3 & 4 & & n \end{bmatrix}$$

8. Find the determinant and inverse of the matrix over there →.

$$\det = 1 \qquad \text{Inv.} = \begin{bmatrix} 2 & -1 & & \\ -1 & 2 & -1 & \\ & -1 & & \end{bmatrix}$$

Jan 1987

Algebra General Exam

1. Show (by Sylow theory) that a group of order 72 cannot be simple. List all abelian groups of order 72.

2. Let G be an infinite group containing an element $x \neq 1$ having only finitely many conjugates. Prove that G is not simple.

3. Let $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$. Find the splitting field F of f(x) over $\mathbb{Q}$, determine its Galois group, and find all subfields of F.

4. Let $k \subseteq K \subseteq L$ and let $\alpha \in L$. Assume that K/k is finite algebraic.
   (a) Show that K/k separable $\Rightarrow$ $K(\alpha)/k(\alpha)$ separable.
   (b) Show that K/k normal $\Rightarrow$ $K(\alpha)/k(\alpha)$ normal.
   (c) Show that if K/k is Galois, then so is $K(\alpha)/k(\alpha)$ and compare the Galois groups $G(K/k)$ and $G(K(\alpha)/k(\alpha))$.

5. What are necessary and sufficient conditions on the commutative integral domain R in order that the polynomial ring in one indeterminate, R[x], be
   (a) a P.I.D.?
   (b) a UFD?
   (c) a Noetherian ring?

6. Let R be a commutative ring with unit and I an ideal of R. Consider the R-module R/I.

   (a) Show that if I is a prime ideal, then R/I is indecomposable.

   (b) Show that R/I is a simple module if and only if I is maximal.

7. Let T be a linear transformation of $\mathbb{R}^5$ having characteristic polynomial T^5-T. Find its possible rational canonical forms over $\mathbb{R}$ and its possible Jordan canonical forms over $\mathbb{C}$.

ALGEBRA GENERAL EXAMINATION - FALL 1987

****

1. Show that a group of order 160 having two subgroups of order 80 also has a normal subgroup of order 5.

2. Prove or disprove: If R is a principal ideal domain so is R[x].

3. A complex number satisfying a monic polynomial with integer coefficients is called an algebraic integer. Show that the complex number α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module.

4. Use the properties of tensor products to show $\mathbb{Z}_2 \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_3 = 0$ and $\mathbb{Z}_2 \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_2 \cong \mathbb{Z}_2$.

5. Determine whether the real quadratic forms $Q_i(x) = xA_ix^t$ with $A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix}$ and $A_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ are equivalent.

6. Find the rational canonical form over the real numbers of the linear transformation whose Jordan canonical form is

$$\begin{bmatrix} 2 & 1 & & & & & & \\ 0 & 2 & & & & & & \\ & & 2 & & & & & \\ & & & 2 & 1 & & & \\ & & & 0 & 2 & & & \\ & & & & & i & 1 & \\ & & & & & 0 & i & \\ & & & & & & & -i & 1 \\ & & & & & & & 0 & -i \end{bmatrix}.$$

7. If K is a finite field with 9 elements, determine whether x^2+x-1 has a root in K.

8. Let $K/\mathbb{Q}$ be a splitting field of an irreducible polynomial $f(x)$ of degree 8. Suppose α is a root of f and that f factors over $\mathbb{Q}(\alpha)$ into 2 linear factors and 3 quadratic factors. Find the possible orders of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Show f is solvable by radicals.

Dan King

ALGEBRA GENERAL EXAMINATION

Saturday August 27, 1988

9:00-12:00 AM

CLOSED BOOK. USE YOUR OWN PAPER. WRITE FINAL ANSWERS NEATLY AND LOGICALLY (turn in scratchwork too).

PROBLEM 1.

PROVE that the ring F[X] of polynomials in one variable over a field F is a principal ideal domain.

PROBLEM 2.

Let T be a linear transformation of $\mathbb{R}^6$ (where $\mathbb{R}$ is the field of real numbers) having characteristic polynomial $T^6 - T^5 - T^2 + T$. FIND the possible rational canonical forms for T over $\mathbb{R}$ and the possible Jordan canonical forms over the complex field $\mathbb{C}$.

PROBLEM 3.

Use the properties of tensor products to SHOW

$$Z_2 \otimes Z_5 = 0$$

(Z_n the ring of integers mod n) and

$$Z_5 \otimes Z_5 \cong Z_5.$$

PROBLEM 4.

SHOW, using the Sylow theory, that a group of order 200 cannot be simple. LIST all abelian groups of order 200.

PROBLEM 5.

Let $f(X) = X^4 - X^2 - 6$ over the field Q of rational numbers. FIND the splitting field F of f(X) over Q, DETERMINE its Galois group, and FIND all subfields of F.

PROBLEM 6.

Let R be a commutative ring with unit, and I an ideal of R. Consider R/I as an R-module.

(a) SHOW that R/I is simple as R-module if and only if I is a maximal ideal of R.

(b) SHOW that if I is a prime ideal of R, then R/I is an indecomposable R-module.

(c) If I is a prime ideal in R, what conclusion can you deduce about R/I as a RING?

PROBLEM 7.

PROVE the famous result of Gauss which states that every algebraic integer over Q which is also in Q is in fact an ordinary integer (in Z). [Note: An *algebraic integer* is a complex number which satisfies a monic polynomial with (ordinary) integer coefficients.]

Jake

ALGEBRA GENERAL EXAMINATION

SATURDAY, JANUARY 14, 1989

9:00 - 12:00 AM

CLOSED BOOK. USE YOUR OWN PAPER. WRITE FINAL ANSWERS NEATLY AND LOGICALLY (REWRITE YOUR ROUGH SCRATCHWORK, BUT TURN IT IN TOO) JUSTIFY ALL YOUR ANSWERS!

PROBLEM 1. Show that there are no simple groups of order 1989.

PROBLEM 2. a) Suppose that G is a group having a factor group G/N isomorphic to the integers Z. Show that for each integer $n > 0$ there exists a normal subgroup H of G having index $[G:H] = n$.

b) Prove or disprove: if all proper factor groups G/N of N ($N \neq \{1\}$) are finite, then G itself is finite.

PROBLEM 3. Let F be a field, and $R = F[[X]]$ the ring of formal power series $f(X) = a_0 + a_1X + a_2X^2 + \ldots$ in the indeterminate X with coefficients a_i from F.

a) Find all *units* (invertible elements) in R.

b) Show that each element f of R is an *associate* of X^n for some n (i.e. $f = X^n g$ for a unit g of R).

c) Find all *irreducible* elements of R.

d) Show that all *ideals* I of R have the form $I = \langle X^n \rangle$ for some n. (i.e. $I = R \cdot X^n = \{fX^n \mid f \in R\}$).

e) Describe all finitely-generated R-modules.

PROBLEM 4. a) Find the Galois group of the equation $x^3 - 2 = 0$ over the field Q of rational numbers.

b) Find a polynomial $f(X) \in Q[x]$ with Galois group $Z_2 \times S_3$ over Q.

PROBLEM 5. If T is a linear transformation on a 9-dimensional complex vector space V with minimum polynomial $m_T(X) = X^2(X-1)^2(X+1)^3$, find the number of possible Jordan canonical forms for T.

PROBLEM 6 (Kummer's Dilemma) Prove or disprove: every Unique Factorization Domain is a Principal Ideal Domain.

That's All, Folks!

Algebra General Examination, May 25, 1989, 9-12.

1. Find the rational and Jordan canonical forms (over $\mathbb{C}$) of $\begin{bmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{bmatrix}$.

2. Show that in a ring, all the elements that are not divisors of zero have the same additive order. What are possible values for this order?

3. Let F be a field and a and b elements of an extension of F that are both algebraic over F, a having degree m and b degree n. Show that $[F(a,b) : F] \leq mn$, with equality if m and n are relatively prime. Find an example giving strict inequality if m and n are not relatively prime.

4. Let $B = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}$ with entries in $GF(3)$, the field of three elements. Find a matrix P for which PBP^T is diagonal.

5. Let H and K be subgroups of a group G. The H-K double coset determined by $g \in G$ is the set $HgK = \{hgk \mid h \in H, k \in K\}$. Prove that two double cosets are either equal or disjoint.

6. Let E/F be a finite Galois extension whose Galois group is simple. Let $a \in E$, $a \notin F$, and let $f(x)$ be the minimal polynomial of a over F. Show that E is a splitting field of $f(x)$.

7. Let R be a commutative ring and let J be the intersection of all maximal ideals of R. Show that $a \in J$ if and only if $1+ta$ is a unit for all $t \in R$. (Any proper ideal of R is in a maximal ideal.)

8. Let G be a finite group and H a normal subgroup. Let P be a Sylow subgroup of H for some prime. Let N be the normalizer of P, $N = \{g \in G \mid gPg^{-1} = P\}$. Prove that $G = HN$.

9. Let A be a square matrix with entries in the field F. Suppose one of the elementary divisors of A is $\lambda - a$ for some $a \in F$. Prove that there is a matrix Q for which QAQ^{-1} is in rational canonical form and $\det Q = 1$. (You may assume the unqualified rational canonical form theorem.)

Algebra General Examination, Tuesday, Aug. 29, 1989
9 – 12 AM

1. What is the class equation for a finite group? Use it to prove that a non-trivial p-group (one whose order is a power of the prime p) has a non-trivial center.

2. Let R be a ring in which $(a+b)^2 = a^2+b^2$ for all a and b in R. Show that R is commutative.

3. Prove that the set of matrices $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ for a, b in GF(5) forms a field, under the usual matrix operations) of size 25.

4. Show that the set T of polynomials in $\mathbb{Z}[x]$ for which the coefficient of x is even forms a subring. Show that in T, 2 and 2x have a greatest common divisor all right, but not a least common multiple.

5. Let E be an extension field of the field F, with [E:F] finite. Prove that any endomorphism of E leaving the members of F fixed is an automorphism.

6. Find the order of the additive Abelian group generated by a, b, and c, subject to the relations

$$\begin{aligned} -4a + 2b + 6c &= 0 \\ -6a + 2b + 6c &= 0 \\ 7a + 4b + 15c &= 0. \end{aligned}$$

Is it cyclic?

7. List the possible rational canonical forms for 2 by 2 matrices over GF(2).

8. Let $\alpha = \sqrt{2+\sqrt{2}}$. Show that $\mathbb{Q}(\alpha)$ is a Galois extension of $\mathbb{Q}$ and that its Galois group is cyclic. Set up the Galois correspondence.

GENERAL EXAM IN ALGEBRA
FRIDAY, MAY 18, 1990

CLOSED BOOK 3 + ε HOUR TIME LIMIT

SHOW ALL!!! WORK ON SEPARATE SHEETS OF PAPER (ONE SHEET FOR EACH PROBLEM). YOU CAN HAVE EXTRA TIME AT THE END TO WRITE UP YOUR SCRIBBLINGS IN A NEAT AND TIDY FASHION, BUT TURN IN THE SCRIBBLINGS ANYWAY.

1. Show that a group which has no nontrivial automorphisms must have order ≤ 2.

2. Show that a group of order 441 must be solvable.

3. If E is a subfield of the complex numbers and a finite Galois extension of the field Q of rational numbers whose Galois group G(E/Q) is simple of order greater than 2, show E cannot contain the complex number i.

4. Show that in a Unique Factorization Domain the following two conditions on a nonzero prime ideal P are equivalent: (1) P is minimal among all nonzero prime ideals, (2) P is a principal ideal.

5. If R is an integral domain having only finitely many ideals, show that R is a field, and give an upper bound for the number of ideals

6. Let R be a principal ideal domain. Show (1) $\mathrm{Hom}_R(M_1 \oplus M_2, N) \cong \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N)$ for any R-modules M_1, M_2, N, (2) $\mathrm{Hom}_R(R,R) \cong R$, (3) if M is finitely generated then its "dual" $\mathrm{Hom}_R(M,R)$ is free of finite rank.

7. Decide which of the following 8×8 matrices are similar over the complex numbers, and explain why.

(1)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & -3 & 0 & -3 & 0 \end{pmatrix}$$

(2)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -i & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -i & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i \end{pmatrix}$$

(3)

$$\begin{pmatrix} i & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & i & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -i & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Algebra General Exam
May 22, 1991

Closed book. Write your final answers neatly
(turn in your scratchwork).

****

I. Let T be a linear transformation on the finite-dimensional vector space V over the field $\mathbb{R}$ of real numbers into itself. Suppose the minimum polynomial for T is T^4+T^2.

(a) If dim V = 6, what are the possible rational canonical forms for T?

(b) If the field of scalars is extended to the complex field $\mathbb{C}$, and dim V = 6, what are the possible Jordan canonical forms for T.

(c) Suppose T has the property that $\text{Trace}(T^k) = 0$ for all $k > 0$, and the minimal polynomial of T divides T^4+T^2. Show that T is nilpotent.

II. Let R be a Euclidean integral domain.

(a) Show that R is a principal ideal domain and that any two non-zero elements of R have a greatest common divisor (g.c.d.) in R.

(b) Is the polynomial ring R[x] a Euclidean integral domain and/or do two non-zero elements of R[x] have a g.c.d. in R[x]? Give <u>reasons</u> for your answers.

III. Given the two quadratic forms $Q_i(x) = xA_ix^t$ where

$$A_1 = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}$$

(a) are they equivalent forms over the rational field, $\mathbb{Q}$?

(b) are they orthogonally equivalent over the real field, $\mathbb{R}$?

IV. (a) Determine the structure of all abelian groups of order 4851.

(b) Let G be a group of order 231. Show that the 11-Sylow subgroup, H, of G is normal in G and lies in the center of G. (Hint: Let G act on H by conjugation.)

V. Let K be the splitting field of x^4-2 over the rational field $\mathbb{Q}$.

(a) Find the Galois group of x^4-2 over $\mathbb{Q}$.

(b) Identify the subfields of K of degree 4 over $\mathbb{Q}$ and find their corresponding subgroups of the Galois group.

VI. Let $M = \mathbb{Z}\oplus\mathbb{Z}$ be the free module of rank 2 over the ring, $\mathbb{Z}$, of integers. Let S be the submodule of M spanned by $x = (3,0)$, $y = (0,4)$, and $(6,2)$. Find a $\mathbb{Z}$-basis for the submodule S.

Algebra General Exam
January 1992

Closed book. Write your final answers neatly (turn in your scratch work). Three hour time limit.

****

1. Prove: An infinite abelian group is cyclic if and only if every subgroup other than $\{1\}$ has finite index.

2. Show that a polynomial of degree n over a field F has at most n roots in F.

3. For $\mathbb{Q}$ the rationals and ω a primitive cube root of 1, determine whether $\mathbb{Q}(\omega\sqrt[3]{2})$ is a Galois extension of $\mathbb{Q}$. Give reasons.

4. Prove: If a finite group G has a normal p–Sylow subgroup S_p, then $\varphi(S_p) \subset S_p$ for every endomorphism φ of G.

5. A matrix E is idempotent if $E^2 = E$. Show that two idempotent matrices over a field are similar if and only if they have the same rank.

6. Prove: An integral domain has the descending chain condition on ideals if and only if it is a field.

7. Apply the Jordan–Hölder–Schreier Theorem on composition series to a finite cyclic group of order n to prove that n has a unique factorization as a product of primes.

Algebra General Exam
May 1992

Closed book. Write your final answers neatly (turn in your scratch work). Three hour time limit.

****

1. Show that an abelian group has a composition series if and only if it is finite.

2. Show that if $a^n = b^n$ and $a^m = b^m$ for m and n relatively prime positive integers and a and b in a commutative integral domain, then $a = b$.

3. Let V be the subgroup $\{1,(12)(34),(13)(24),(14)(23)\}$ of the symmetric group S_4 on 4 symbols. Prove that V is a normal subgroup of S_4 and that $S_4/V \cong S_3$.

4. Give the Jordan normal forms for all 6×6 matrices, over the complex numbers, whose minimal polynomials are $(x-1)^2(x-2)$.

5. The Euler φ–function on the natural numbers is given by: $\varphi(n)$ = the number of integers x with $1 \leq x \leq n$ and x relatively prime to n. It is a fact that $n = \sum_{d|n} \varphi(d)$. Explain this in terms of the subgroup structure of the cyclic group of order n.

6. Show that $f(x,y) = x + x^3y + y^8 + x^7y^5 + x^2y^4$ is irreducible over the rational field.

7. Show that if a 2×2 real symmetric matrix A has $\lim_{n \to \infty} \text{trace}(A^n) = 0$, then $\lim_{n \to \infty} A^n = 0$. Does this hold for $n \times n$ real symmetric matrices?

Algebra General Examination
September 4, 1993

This is a closed book exam. Please write your answers neatly and turn in your scratch work. The allowed time is three hours. There are 7 problems.

1. A real square matrix T is called tripotent if $T^3 = T$. Show that two tripotent matrices of the same size are similar if and only if they have the same rank and the same trace.

2. Let R be a commutative ring and let P be a prime ideal of R. Show that if P is not maximal, then P has infinitely many cosets in R.

3. Let N be a normal subgroup of the finite group G, and let P be a p-Sylow subgroup of N for some prime p. By considering conjugates of P, prove that if the normalizer of P is H, then $G = HN$.

4. Prove that it can never be the case that the additive group of a field is isomorphic to the multiplicative group of nonzero elements. [Hint: consider orders of elements in the two groups.]

CONTINUED ON THE REVERSE

5. a) Let D be a Euclidean domain, with Euclidean function δ (but do not assume $\delta(ab) \geq \delta(a)$). Let $D_n = \{a \in D \mid a \neq 0 \text{ and } \delta(a) \geq n\}$. Show that

1) if $b \in D_0$ and there exists an $a \in D$ such that $a + Db \subseteq D_n$, then $b \in D_{n+1}$;

2) $\bigcap_n D_n = \emptyset$.

b) Conversely, show that if an integral domain D has a chain of subsets $D - \{0\} = D_0 \supseteq D_1 \supseteq D_2 \supseteq \cdots$ satisfying properties 1) and 2), then D is Euclidean.

6. Let $f(x) = x^5 - 6x + 3$.

a) Prove that $f(x)$ is irreducible over the rational field, $\mathbb{Q}$.

b) Prove that $f(x)$ has exactly three real roots.

c) Let F be the splitting field of $f(x)$ over $\mathbb{Q}$. If E is a real subfield of F, prove that the Galois group, $\mathcal{G}(F/E)$, of F over E contains a transposition (in the action on the roots of $f(x)$).

d) $\mathcal{G}(F/\mathbb{Q})$ is isomorphic to S_5. Assuming that, prove that if $r \in \mathbb{Q}$ is positive, but $\sqrt{r} \notin \mathbb{Q}$, then $\sqrt{r} \notin F$.

7. In a well-known puzzle (figure a) one can move the tiles, numbered 1 to 15, so that at the end of a sequence of moves, the empty square is again at the lower right (figure b). The numbers 1 to 15 have been permuted by $\pi \in S_{15}$. Show that $\pi \in A_{15}$.

(An allowable move consists of sliding a tile, adjacent to the empty square, horizontally or vertically, into the position of the empty square.)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(a)

$\pi(1)$	$\pi(2)$	$\pi(3)$	$\pi(4)$
$\pi(5)$	$\pi(6)$	$\pi(7)$	$\pi(8)$
$\pi(9)$	$\pi(10)$	$\pi(11)$	$\pi(12)$
$\pi(13)$	$\pi(14)$	$\pi(15)$	

(b)

ALGEBRA GENERAL EXAMINATION

AUGUST 27, 1994

The examination is closed book. Please write out your answers neatly and include your scratch work. The allowed time is three hours and there are eight problems.

1. Let P be a p-Sylow subgroup of a finite group G, p a prime dividing the order of G.
(a) Prove that P consists of all the p-torsion elements of the normalizer $N_G(P)$, that is, all elements of $N_G(P)$ whose order is a power of p. [Hint: apply Sylow theorems to $N_G(P)$.]
(b) Prove that P is a characteristic subgroup of $N_G(P)$.
(c) Prove that $N_G(N_G(P)) = N_G(P)$.

2. If G is a finite Abelian group of order n, show that G has a subgroup of order d for each divisor d of n. Show that this need not be true if G is not Abelian.

3. Describe the subring $\mathbf{R}[x^2, x^3]$ of the polynomial ring $\mathbf{R}[x]$; that is, specify what polynomials belong to it.

4(a). Find the Jordan form of

$$A = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 2 & -1 & 3 \end{pmatrix}$$

over $\mathbf{C}$.
4(b). If $A \in M_n(\mathbf{C})$ has finite order d, so that d is the smallest positive exponent for which $A^d = I$, describe the Jordan form of A over $\mathbf{C}$.

5. If $f(x, y)$ is an alternating bilinear form on a 25-dimensional real vector space and A is its matrix with respect to some basis, show that $det(A)^{25} = 0$.

6. Show that $F = \mathbf{Z}_2[x]/(x^4 + x + 1)$ is a field of characteristic 2 containing a primitive 15-th root of unity. Exhibit such a root.

OVER

7. Let ζ_n be a primitive n-th root of unity in $\mathbf{C}$ for $n > 2$.
(a) Show that the fixed field of $\mathbf{Q}(\zeta_n)$ under complex conjugation is $\mathbf{Q}(\zeta_n + \bar{\zeta}_n) = \mathbf{Q}(\zeta_n) \cap \mathbf{R}$. [Hint: write $\bar{\zeta}_n$ as a power of ζ_n and find a polynomial of low degree satisfied by ζ_n over $\mathbf{Q}(\zeta_n + \bar{\zeta}_n)$.]
(b) For $n = 7$, find the Galois group of $\mathbf{Q}(\zeta_7 + \bar{\zeta}_7)$. Then find all subfields of $\mathbf{Q}(\zeta_7)$ and their Galois groups.

8. If the annihilator of a left R-module M is $Ann_R(M) = \{a \in R \mid aM = 0\}$, show that for submodules M_1, M_2 of M, we have

$$Ann_R(M_1 + M_2) = Ann_R(M_1) \cap Ann_R(M_2).$$

Show furthermore that we have

$$Ann_R(M_1) + Ann_R(M_2) \subset Ann_R(M_1 \cap M_2);$$

but show that this inclusion could be strict.

ALGEBRA GENERAL EXAMINATION

January 15, 1994

The examination is closed book. Please write out your answers neatly and include your scratch work. The allowed time is three hours; there are eight problems.

1. Find all the possible rational canonical forms for a 5 by 5 matrix with rational entries whose minimal polynomial is $(x-2)^2(x+3)$. Identify a pair having the same characteristic polynomial.

2. Prove that the Galois group of x^4-2 over the rational field is isomorphic to the dihedral group of order 8.

3. Prove that $y^3+x^2y^2+x^3y+x$ is irreducible in $\mathbb{Z}[x,y]$.

4. Let G and H be finite groups and let $f: G \to H$ be a surjective homomorphism. Let p be a prime.
   (a) Prove that if P is a p-Sylow subgroup of G, then f(P) is a p-Sylow subgroup of H.
   (b) Prove that every p-Sylow subgroup of H has the form f(P) for some p-Sylow subgroup P of G.

OVER

5. Give an example (and a proof that it works) of a ring R without identity and an ideal in the direct sum $R \oplus R$ that does <u>not</u> have the form $I_1 \oplus I_2$, where I_1 and I_2 are ideals in R.

6. (a) Explain why the inner automorphism group of the alternating group A_n is isomorphic to A_n for $n \geq 4$.

(b) Prove that for $n \geq 3$, A_n has outer automorphisms.

7. In a field, it is true that if $t^m = 1$ and $t^n = 1$ for two relatively prime exponents m and n, then $t = 1$. Explain how this implies the following result for an integral domain: if $a^m = b^m$ and $a^n = b^n$ for two relatively prime positive exponents m and n, then $a = b$.

8. Let R be a commutative ring with identity and let D be the set of zero divisors of R, including 0. Let $\mathcal{A}$ be the set of ideals of R that are contained in D.

(a) Show that if M is a maximal member of $\mathcal{A}$, then M is a prime ideal.

(b) Use Zorn's lemma to show that each member of D is contained in a maximal member of $\mathcal{A}$.

(c) Conclude that D is a union of prime ideals.

ALGEBRA GENERAL EXAMINATION

JANUARY 28, 1995

This examination is closed book. Please write your answers out neatly and include all your scratch work. The time allowed is three hours, and there are eight problems.

1. In keeping with tradition, let G be a group of order 1995. Show that G must be solvable. (Although you needn't prove them here, you may use only theorems you are able to prove!)

2. Explain the connection between the Fundamental Theorem of Arithmetic and the Jordan-Hölder Theorem applied to cyclic groups.

3. Let K and L be finite extensions of a field F, both contained in a field E. Let KL be the set of sums of products of members of K and L.

Explain why KL is a subring of E that is finite dimensional over F. From that, show that KL is a field and, in fact, the smallest subfield of E containing K and L.

4. List all the possible Jordan canonical forms for a matrix over the complex field whose characteristic polynomial is $x^8 - x^4$ and whose minimal polynomial is $x^6 - x^2$.

5. Give definitions of the terms "maximal subgroup" and "minimal subgroup" - it is not assumed that you have seen these terms explicitly. Then from your definitions, prove the following facts:

a) A minimal subgroup must be cyclic of prime order.
b) If a subgroup has prime index, it is a maximal subgroup.
c) If a subgroup is both maximal and normal, it has prime index.
d) A subgroup of an Abelian group is maximal if and only if it has prime index.

Now find the maximal and minimal subgroups of $\mathbb{Z}$.

6. Prove that any proper homomorphic image of a principal ideal domain that is an integral domain must actually be a field.

Use this result to show that $F[x, y]$, F a field, is <u>not</u> a principal ideal domain.

OVER

7. Show that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$. Label its roots in some way and display the Galois group as a set of permutations of the roots.

8. Give an example of a polynomial $f(x)$ in $\mathbb{Q}[x]$ having all these properties:

a) the degree of $f(x)$ is 4;
b) $f(x)$ has no rational roots;
c) $f(x)$ has no repeated factors in $\mathbb{Q}[x]$;
d) the Galois group of $f(x)$ over $\mathbb{Q}$ is cyclic of order 2.

Algebra Comprehensive Exam

August, 1995

1. Describe a nonabelian group of order 55 as semidirect product, and, using your description, explicitly give generators and defining relations for the group.

2. Let ρ_1: $G \to \text{Aut}(V)$, ρ_2: $G \to \text{Aut}(W)$ be linear representations of a finite group G. Let $L: V \to W$ be a linear map. Show that the linear map L': $V \to W$, defined by

$$L'v = (1/|G|) \Sigma_{g \in G} \rho_2(g^{-1}) L \rho_1(g) v, \quad v \text{ in } V,$$

is an intertwiner of the representations ρ_1 and ρ_2, i.e. $L'\rho_1(g) = \rho_2(g) L'$, for all $g \in G$.

3. Let G be the Galois group of $x^4 - 4$ over the field $\mathbf{Q}$ of rational numbers and let F be the splitting field of $x^4 - 4$. Find G and describe the action of each of its elements on F. Also find all subfields of F.

4. If T is a diagonalizable linear operator on a finite dimensional vector space V, and if W is a T-invariant subspace of V, prove there is a T-invariant subspace U such that $V = W \oplus U$.

5. Factor the polynomial $x^9 - x$ in $\mathbf{F}_3[x]$ into irreducible factors. ($\mathbf{F}_3$ is the field with three elements.)

6. Assume T is a linear operator on a 10-dimensional real vector space V with minimum polynomial $(x^4 - 1)^2$, and let k denote the maximum number of linearly independent eigenvectors of T in V. What are the possible values of k? Justify your answer.

7. Find the order of the group $GL(n, \mathbf{F}_p)$, and describe a p-Sylow subgroup. (p is a prime number, and $\mathbf{F}_p$ is the field with p elements.)

8. A representation of the symmetric group S_3 in the vector space $\mathbf{R}^3$ is defined by letting a permutation in S_3 act on a vector in $\mathbf{R}^3$ by permuting the coordinates of the vector. Express $\mathbf{R}^3$ as a direct sum of irreducible S_3-invariant subspaces. Prove that your direct summands are irreducible S_3-invariant subspaces.

9. List the conjugacy classes of finite subgroups of the orthogonal group $O(2, \mathbf{R})$, and prove your list is correct.

10. The space $M_n(\mathbf{R})$ of $n \times n$ real matrices is a real inner product space with inner product given by: $\langle A, B \rangle = \text{trace}(AB^t)$, where B^t denotes the transpose of the matrix B. (You don't need to prove this.) Let P be an invertible matrix and T the linear operator on $M_n(\mathbf{R})$ defined by $T(A) = P^tAP$. Denote the adjoint of T by T*. Prove that $T^*(A) = PAP^t$, and find necessary and sufficient conditions on the matrix P that $T = T^*$. Justify your answer.

ALGEBRA GENERAL EXAMINATION

AUGUST 26, 1995

This algebra examination is closed book. Please write your answers out neatly and include all your scratch work. The time allowed is three hours, and there are seven problems altogether.

1. Let G be a finite group of permutations of the finite set X. For $x \in X$, let

$$G_x = Stab(x) = \{g \in G : gx = x\}.$$

Suppose $| X | = [G : G_x]$ for some $x \in X$. Show this holds for <u>all</u> $x \in X$.

2. Let G be a group of order 1001. Show:

a) G is not simple;

b) G is Abelian;

c) G is cyclic.

3. Let A be the Abelian group (written additively) generated by x_1, x_2, x_3 satisfying the relations

$$\begin{aligned} 4x_1 - 2x_2 + 4x_3 &= 0 \\ 7x_1 - 8x_2 + x_3 &= 0 \\ 8x_1 + x_2 + 13x_3 &= 0 \end{aligned}$$

Find the order of A.

4. Show that $\mathbb{Z}[\sqrt{10}] = \mathbb{Z} + \mathbb{Z}\sqrt{10}$ is not a factorial (unique factorization) domain. Hint: show that

a) $n^2 - 10m^2 \neq 2, 3$ for all $n, m \in \mathbb{Z}$.

b) 2, 3, and $4 \pm \sqrt{10}$ are primes in $\mathbb{Z}[\sqrt{10}]$.

5. Find the Jordan canonical form of the $n \times n$ matrix $A = (a_{ij})$ with $a_{ij} = 1$ for $i \leq j$ and $a_{ij} = 0$ for $i > j$.

OVER

6. Let $K/\mathbb{Q}$ be a splitting field of $x^3 - 9x + 12$. Show that there is a single normal extension $L/\mathbb{Q}$ in K with $\mathbb{Q} \neq L \neq K$. Find $[L : \mathbb{Q}]$.

7. Show that every element of $SO_5(\mathbb{R})$ has a fixed point ($Ax = x$ for some $x \neq 0$). Recall that

$$SO_5(\mathbb{R}) = \{A \in \mathbb{R}_5 : (Ax, Ay) = (x, y), \text{and } \det A = 1\},$$

where $(x, y) = x \cdot y = x^t y$ is the usual bilinear form (dot product) on $\mathbb{R}^5$.

ALGEBRA GENERAL EXAMINATION

August 24, 1996

Instructions. This algebra examination is closed book. Please write out your answers carefully, being sure to explain any claims you make. Include your scratch work with what you turn in. The time allowed is three hours, and there are eight questions.

1. A Hall subgroup H of a finite group G is a subgroup whose order and index are relatively prime. Use isomorphism theorems to prove that if N is a normal subgroup of G and H is a Hall subgroup of G, then HN/N is a Hall subgroup of G/N, and $H \cap N$ is a Hall subgroup of N.

2. Let C_n denote the cyclic group of order n. Determine all pairs of positive integers a and b, with $a \leq b$, for which $C_a \times C_b$ is isomorphic to $C_{15} \times C_{18} \times C_{20}$.

3. Let M be a finitely generated R-module, R a ring. Show that any generating set of M (a subset of M that generates M as an R-module) must contain a finite generating set. Conclude that M has a minimal generating set (no proper subset generates M), and that every minimal generating set of M is finite.

4. In $\mathbf{Q}[x]$, let $f(x) = x^{m_1} + \ldots + x^{m_k}$, where $m_i \equiv i - 1 (\mathrm{mod}\, k)$. Show that $f(x)$ is divisible by $x^{k-1} + x^{k-2} + \ldots + 1$.

5. Let R be a principal ideal domain. An ideal P of R is called *primary* if whenever $ab \in P$ and $a \notin P$, then $b^n \in P$ for some n (perhaps depending on b). Show that P is a primary ideal if and only if either $P = \{0\}$ or $P = (p^m)$ for some prime p and exponent m.

6. Let E/F be a finite Galois extension with Galois group G. The normal basis theorem states that there is an element u in E whose images under the members of G form an F-basis of E.

   Prove that for any subgroup H of G, the subfield corresponding to H in the Galois correspondence is $F(u_H)$, where

   $$u_H = \sum_{h \in H} h(u).$$

7. The minimal polynomial of a matrix A with real entries is $(x-1)(x^2+1)^2$ and its characteristic polynomial is $(x-1)^3(x^2+1)^2$.

   (a) What is the rational canonical form of A?

   (b) If A is regarded as having complex entries, what is its rational canonical form?

   (c) What is the Jordan normal form of A (again, with complex entries)?

8. Give an example of two finite groups whose Sylow subgroups are isomorphic for each prime, but which are themselves not isomorphic.

ALGEBRA GENERAL EXAMINATION

January 23, 1997

This algebra examination is closed book. Please write out your answers carefully, being sure to explain any claims you make. Include your scratch work with what you turn in. The allowed time is three hours, and there are seven questions.

1. Find the rational canonical form and the Jordan normal form for the real matrix

$$\begin{pmatrix} -1 & 3 & 0 \\ 0 & 2 & 0 \\ 2 & 1 & -1 \end{pmatrix}.$$

2. Let G be a finite Abelian group of order k. Use the fact that the map $g \to g^n$ (n an integer) is a homomorphism, to show that if k_n is the number of solutions of $g^n = 1$ in G, and $k^{(n)}$ is the number of n-th powers in G, then $k = k_n k^{(n)}$.

3. Let E be a separable extension of the field F, with $[E : F] = n$. Use Galois theory to find an upper bound $B(n)$ for the number of intermediate fields K, $F \subseteq K \subseteq E$, that depends only on n. You don't need to make the bound $B(n)$ very tight!

4. Give counterexamples for each of the following statements, with details. Then correct each statement by modifying the underlined part.

   (a) If R is a commutative ring, a polynomial in $R[x]$ of degree n has at most n roots in R.

   (b) If R is a division ring, a polynomial in $R[x]$ of degree n has at most n roots in R.

   (c) If R is a unique factorization domain, then the greatest common divisor, d, of two members a and b of R can be written as $d = ax + by$ for some x and y in R.

5. Describe the Galois group of $x^4 - 5$ over the rationals as a group of permutations of the roots.

6. Let G be a finite group and P a p-Sylow subgroup of G for the prime p. Prove that if H is a subgroup of G, then for some $g \in G$, $H \cap gPg^{-1}$ is a p-Sylow subgroup of H.

7. Let V be a finite-dimensional vector space over a field F, and let λ and μ be two linear functionals on V. Define

$$B(x, y) = \lambda(x)\mu(y) - \lambda(y)\mu(x)$$

   for x and y in V. Show that B is an alternate (alternating) form on V and determine the possible values for its rank.

Algebra General Examination - Saturday, August 23, 1997; 9 - 12

This examination is closed book. Please explain yourself carefully and clearly; avoid words like "obviously"! Save your scratch-work and turn it in along with the examination. Allow enough time to polish your answers.There are eight problems.

1. Let p be a prime number, and let K be a field containing p distinct p-th roots of unity. Let L/K be a Galois extension for which $[L : K] = p$.

a) Prove that the Galois group $Gal(L/K)$ is cyclic of order p.

b) Let σ be a generator of $Gal(L/K)$. Then σ is a K-linear transformation on the vector space L. What is the Jordan canonical form of σ?

c) Prove that there is an element u in $L - K$ with u^p in K.

2. a) Let G be a finite group with exactly two conjugacy classes of elements. Prove that $|G| = 2$, where $|G|$is the order of G.

b) Suppose that G has exactly three conjugacy classes of elements. Show that $|G|$ involves at most two primes.

c) There are, in fact, only two finite groups with exactly three conjugacy classes of elements. Can you guess which ones they are?

3. Let $K(x)$ be the field of rational functions over the field K. Prove *Lüroth's theorem*: for any nonconstant function, f (that is, $f \in K(x) - K$), the degree $[K(x) : K(f)]$ is finite. Can you describe $[K(x) : K(f)]$ in terms of f ?

4. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. Let p be a prime and let $\overline{f}(x)$ be the image of $f(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ obtained by reducing the coefficients of $f(x)$ modulo p. A theorem of Kronecker says that if $\overline{f}(x)$ has distinct roots in its splitting field, and if $\overline{\sigma}$ is a member of the Galois group of $\overline{f}(x)$ over $\mathbb{Z}/p\mathbb{Z}$, then there is an element σ of the Galois group of $f(x)$ over $\mathbb{Q}$ having the same cycle structure as a permutation of the roots of $f(x)$ as $\overline{\sigma}$ does as a permutation of the roots of $\overline{f}(x)$.

a) Use this theorem (with a couple of choices of p) to show that the Galois group of $x^4 + 4x^2 + x + 3$ is isomorphic to S_4.

b) Apply the theorem to show that if $f(x)$ has even degree and the discriminant of $f(x)$ is a perfect square in $\mathbb{Z}$, then $\overline{f}(x)$ is reducible for each prime p.

5. If g is a member of a group G, then g is called a *nongenerator* of G if whenever G is generated by a subset containing g, it is also generated by the subset with

g removed. It is a fact that the set of all nongenerators of G forms a subgroup; that subgroup is called the *Frattini subgroup* of G.

Suppose that G is a finite p-group, p a prime, and F is the Frattini subgroup of G. Show that $g \in F$ if and only if g is in every subgroup of index p of G. (You may need the fact that if H is a proper subgroup of G, then H is a proper subgroup of its normalizer in G.) Conclude that G/F is an Abelian group of exponent p.

6. Let R be an integral domain and let $N : R - \{0\} \to \{n > 0 \mid n \in \mathbb{Z}\}$ be a function for which $N(1) = 1$ and $N(xy) = N(x)N(y)$, for all x, y in $R - \{0\}$.

a) Let K be the field of fractions of R. Show that N can be extended in a unique way to a function from $K - \{0\}$ into $\mathbb{Q}$ for which $N(xy) = N(x)N(y)$ still holds.

b) Show that R is a Euclidean domain (under N) if and only if for each $x \in K - \{0\}$ there is an element $r \in R$ for which $N(x - r) < 1$.

7. Let M be the free module over $\mathbb{Q}[x]$ with basis v_1, v_2, v_3. A certain submodule N of M has basis w_1, w_2, w_3, with

$$\begin{aligned} w_1 &= (x^3 - x^2 - x + 1)v_1 + (2x^2 + 2x)v_2 + (x^3 + x^2)v_3 \\ w_2 &= (2x^3 - 3x^2 - 3x + 2)v_1 + (5x^2 + 5x)v_2 + (2x^3 + 2x^2)v_3 \\ w_3 &= (x^3 - x)v_1 + (x^2 + x)v_2 + (x^3 + x^2)v_3. \end{aligned}$$

a) There is a theorem which implies that M has a basis b_1, b_2, b_3 for which d_1b_1, d_2b_2, d_3b_3 are a basis for N for some d_1, d_2, d_3 in $\mathbb{Q}[x]$ with d_1 dividing d_2 and d_2 dividing d_3. Write a carefully worded statement of such a theorem, giving all pertinent hypotheses and all appropriate conclusions.

b) Find values for d_1, d_2, d_3 for the example given here.

8. a)Suppose R is a commutative ring with identity and let N be the set of all nilpotent elements of R. Show that N is an ideal; it is called the *nil radical* of R.

b) The intersection of all maximal ideals of R is called the *Jacobson radical* of R. If J is the Jacobson radical of R, show that $N \subseteq J$.

c) Show that $x \in J$ if and only if $1 + x$ is a unit of R. [*Error here: the problem should have said:* $1 + rx$ *is a unit for all* r *in* R.]

d) Give an example for which N and J are different.

ALGEBRA GENERAL EXAMINATION

January 17, 1998

Question 1 (a) What can you say about groups G of the following orders $|G|$? (Give reasons, making free use of any theorems you know.)

(1) $|G| = 2^4 + 1 : G \cong ?$

(2) $|G| = 2^3 + 1 : G \cong ?$

(b) What can you say about *simple* groups G of the following orders $|G|$? (Again, explain your answer.)

(1) $|G| = 2^m + 1 : G \cong ?$

(2) $|G| = 2.3.5 : G \cong ?$

(3) $|G| = 2^2.3.5 : G \cong ?$

All your answers should be quite short.

Question 2 (a) How many non-isomorphic abelian groups are there of order 360?

(b) Take the free abelian group on generators x, y and z. Divide it by the relations

$$\begin{aligned} 2x + 4y + 5z &= 0 \\ 6x + 8y + 10z &= 0 \\ 8x + 12y + 20z &= 0 \end{aligned}$$

Write the resulting group as a direct sum of cyclic groups.

Question 3 Let R be a principal ideal domain. Suppose a and b are two non–zero elements in R. Show that they have a least common multiple. That means the following. We adopt the notation that $a \mid m$ means "a divides m". You need to show that there exists an element $m \in R$, so that

3.1 $a \mid m$ and $b \mid m$.

3.2 If $a \mid x$ and $b \mid x$, then $m \mid x$.

Question 4 Let M be a module over a ring. A *section* $A : B$ of M is a pair of submodules A, B of M with $B \subseteq A$; a *trivial section* is where $B = A$. A submodule C of M *covers* a section $A : B$ if $(A \cap C) + B = A$, and *avoids* $A : B$ if $A \cap C \subseteq B$.

Algebra General Exam August 22, 1998

This is exam is worth 100 points. The number of points each part of a problem is worth is indicated in brackets. If you can't prove part of some problem, you can still use the result of that part in proving subsequent parts.

(1)[20] Let G be a finite group of order $3 \cdot 5 \cdot 17$.

(a)[5] Show that the Sylow 17-subgroup is normal.

(b)[5] *If there exists an element of order 15 in G,* show that the Sylow 3- and 5-subgroups are also normal. [Hint: show they are properly contained in their normalizers.]

(c)[5] If all Sylow subgroups of a finite group G are normal and abelian, show that G itself is abelian.

(d)[5] If G is a finite abelian group of order $p \cdot q \cdot r$ for distinct primes p, q, r, show that G is cyclic.

(2)[15] Let $GL_2(p)$ for a prime p denote the group of invertible 2×2 matrices over the finite field F_p of p elements.

(a)[5] Find the order n of the group $GL_2(p)$.

(b)[5] For λ in F_p, the find the order m of the subgroup

$$G_\lambda = \{A \in GL_2(p) \mid A \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} A^{-1} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}\}.$$

(c)[5] Find how many 2×2 matrices over F_p are similar to the matrix $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. [Hint: express it in terms of m and n.]

(3)[10] For an abelian group A, the *dual group* A^* is defined to be $Hom(A, U)$ where the *circle group* U is the multiplicative group of complex numbers of modulus 1 (the unit circle in the complex plane). Here $Hom(A, B)$ denotes the abelian group of homomorphisms of A into B (under $(f+g)(a) = f(a) + g(a)$); you may use the additivity property $Hom(A_1 \oplus A_2, B) \cong Hom(A_1, B) \oplus Hom(A_2, B)$ and the isomorphism property that if $A \cong A', B \cong B'$ then $Hom(A, B) \cong Hom(A', B')$.

(a)[5] Prove that Z_n^* is cyclic of order n.

(b)[5] Prove that A^* is isomorphic to A for *any* finite abelian group A.

(4)[10] Let a, b, c be distinct elements of an integral domain D. Show that there are *unique* elements x, y, z in D such that

$$\begin{aligned} x + y + z &= 0 \\ ax + by + cz &= 0 \\ a^2x + b^2y + c^2z &= 0 \end{aligned}.$$

Algebra General Exam August 21, 1999

This is exam is worth 100 points. The number of points each part of a problem is worth is indicated in brackets. If you can't prove part of some problem, you can still use the result of that part in proving subsequent parts.

(1)[10] Let P be a p-Sylow subgroup of a finite group G for some prime p dividing the group order. We know by Sylow theory that the index of the normalizer of P is congruent to 1 modulo p,

$$[G : N_G(P)] \equiv 1 \pmod{p}.$$

Show that the same holds for any larger subgroup M: if $G \supseteq M \supseteq N_G(P)$ then

$$[G : M] \equiv 1 \pmod{p}.$$

[Hint: show $N_M(P) = N_G(P)$.]

(2)[20] (a)[5] Show that any finite group G has a faithful action on some set S of cardinality $|S| = |G|$.

From now on (in parts b,c) assume that G is a finite p-group for a prime p, having the property that it has a *unique* subgroup G_p of order p. [The quaternion group is such a group, with $p = 2$ and $G_2 = \{1, -1\}$.]

(b)[5] Show that G_p is invariant under all endomorphisms of G, $f(G_p) \subseteq G_p$ for all homomorphisms $f : G \to G$.

(c)[10] Show that G_p "needs room" in order to act: whenever G acts on a finite set S of size $|S| < |G|$, the subgroup G_p acts trivially. Conclude that G can only act faithfully on sets of size $\geq |G|$.

(3)[10] The *exponent* e of a group G is defined as the smallest positive integer k such that $x^k = 1$ for all $x \in G$; for an abelian group, in additive notation this is the smallest k such that $kx = 0$ for all elements. If $n_1, n_2, \ldots, n_r$ are the invariant factors of a finite abelian group A (so $n_r | n_{r-1} | \ldots | n_2 | n_1$), *prove* that A has exponent $e = n_1$, and has an element of order precisely e. Conclude that A has an element of order m iff m divides the largest invariant factor n_1.

General Exam-Algebra
August 14th, 2000

1. Let V be a non-zero vector space over the field of reals R. Show that V cannot be presented as the union of three proper subspaces.

2. For a field K, we denote by K(x) the field of rational functions in one variable x over K. Prove that C(x) is not the algebraic closure of R(x). (R is the real numbers and C the complex numbers.)

3. (i). Let G be a finite group of order $p^\alpha m$ where p is a prime relatively prime to m, and let G_p denote the set of elements of G whose order is p^i for some $i>0$. Show that

$|G_p| \leq [G:N](p^\alpha-1)$ where N is the normalizer of some Sylow p-subgroup, with equality holding iff any two distinct Sylow p-subgroups have trivial intersection.

(ii). Let G be a finite group of order $p^\alpha q^\beta$ for distinct primes p and q. Assume that G does not have elements of order pq, and that G has just 1 Sylow q-subgroup.

Show that $|G_p|=q^\beta(p^\alpha-1)$.

Show that any two distinct Sylow p-subgroups have only the identity in common.

4. Let A denote the set of complex numbers of the form $a+b\sqrt{-6}$, with $a, b \in Z$.

(i) Show that A is a subring of C.

(ii) Let J be the ideal of A generated by 5 and $2+\sqrt{-6}$. Show that $J \neq A$.

(iii) Show that J is prime.

(iv) Show that the ideal 5A is not prime.

5. Let A be a commutative ring with 1. Show that $A[x, x^{-1}]$ is Noetherian if and only if A is. (Reminder. A Noetherian ring is one in which every ideal is finitely generated. You may use any characterization of a Noetherian ring you know; you do not need to justify it.)

6. Let R be a ring with 1 and suppose that N is a non-zero left R-module. Show that N is indecomposable if and only if $Hom_R(N,N)$ does not contain an idempotent e with $e\neq 0$ and $e\neq 1$. (Reminders. A module is indecomposable if it not the direct sum of two non-zero submodules. An element s of a ring is idempotent if $s^2=s$.)

7. Let K be a Galois extension of Q, the rational numbers, with the Galois group G(K:Q) isomorphic to A_4. (A_4 is the group of even permutations of 4 objects.)

(i) What is the degree of K over Q?

(ii) Show that there is a polynomial f of degree 4 so that K is isomorphic to the splitting field of f over Q.

Let r_1,r_2,r_3,r_4 be the roots of f in K. Let $\Delta=\prod_{1\leq i<j\leq 4}(r_i - r_j)$.

(iii) Show that Δ^2 is in Q.

(iv) Is Δ in Q? Why or why not?

8. A certain Z-module M is generated by elements a,b, and c. Furthermore $2a+4b+2c=0$, $4a+4b+4c=0$, and $2a+4b+14c=0$. Assume all other Z-combinations of a,b,c which are 0 can be derived from these three. (i.e. these are the defining relations for the module.) Find the invariant factors for this module and describe M up to isomorphism as a direct sum of cyclic submodules.

9. Let X be an invertible matrix with complex entries and let $Y=X^{-1}$.

(i). Show that if λ is an eigenvalue for X then λ^{-1} is an eigenvalue for Y.

(ii). Show that if the Jordan canonical form of X has a kxk Jordan block with diagonal entries λ, then the Jordan canonical form of Y has a kxk Jordan block with diagonal entries λ^{-1}.

Algebra, April 1977

1. Let C be the field of complex numbers, and let A be an $n \times n$ matrix over C. As usual, we define $e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!} = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots$, where the convergence of the series is that of C^{n^2}.

   (a) Use the Jordan canonical form to show that $\det e^A = e^{TrA}$.

   (b) If $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, what is e^A?

2. Let k be a field of q elements where q is finite.

   (a) Show that $q = p^n$ is a power of a prime.

   (b) Show that k is the splitting field of the equation $x^q - x = 0$ and thus is the unique field of q elements.

   (c) The multiplicative group k^* of non-zero elements of k satisfy the equation $x^{q-1} - 1 = 0$. Why does this imply that k^* is a *cyclic* group of order $q - 1$?

3. Use the fundamental theorem for abelian groups to show that in the ring of integers mod p^n, for p an odd prime, the multiplicative group of integers relatively prime to p has a subgroup of order p if $n > 1$.

4. Let R be a commutative ring with 1 and let M be a maximal ideal in R. Show that R/M is a field.

   (a) Show that if R is a Euclidean Integral Domain then every ideal generated by an irreducible element is maximal.

   (b) Let k be a field and $R = k[x]$ the polynomial ring in one variable over k. If $p(x) = p$ is an irreducible polynomial in $k[x]$ use 4. and (a) to show that there is a finite extension K of k in which $p(x)$ has a root.

   (c) If $k = Q$ is the rational field and $p(x) = x^2+x+1$ show that $p(x)$ is indeed irreducible over Q. What is the field generated in (b) for this example?

5. Let $G = S_n$ be the symmetric group on n letters.

   (a) Show that the alternating group A_n on n letters is a normal subgroup of S_n.

   (b) Show that A_n is generated by the three-cycles $(1, 2, i)$,$i = 3, 4, \ldots, n$.

   (c) Show that if H is a normal subgroup of A_n for $n \geq 3$ and H contains a 3-cycle, then

(d) Is the equation $f(x)$ solvable by radical? Give reasons for your answer.

7. Let A be a normal ($A^*A = AA^*$) $n \times n$ complex matrix. Show that there is a polynomial $f(x)$ with complex coefficients such that $A^* = f(A)$. Thus any $n \times n$ matrix B which commutes with A also commutes with A^*. (Assume the spectral theorem for A.)

8. If A and B are algebras over a field k define their tensor product $C = A \otimes_k B$ and show that C is an algebra over k.

   (a) Let A and B each have units and let $Z(A) = Z_1$, $Z(B) = Z_2$, and $Z(C) = Z$ designate the centers of A, B, and C respectively. Show that $Z = Z_1 \otimes Z_2$.

Algebra, November 1977

1. How many non-isomorphic fields are there with exactly 3 elements? Exactly 6 elements? Exactly 9 elements?

2. Describe the following tensor products of modules in more explicit form. (Z = integers).

   (i) $Z_2 \otimes_{Z_4} Z_4$

   (ii) $Z_2 \otimes_Z Z_3$

   (iii) $Z_2 \otimes_{Z_3} Z$

3. Give an example of an *inseparable* extension of degree 7 over Q (the rationals).

4. Define "finite" and "algebraic" extensions of fields. Does algebraic imply finite? Does finite imply algebraic? Prove or give counterexample.

5. Give an example of a non-Noetherian commutative ring.

6. Find all eigenvectors and eigenvalues of the linear operator $D = \frac{d}{dx}$ (differentiation) on the space $V = C^\infty(R)$ of infinitely differentiable complex-valued functions on the real line R. The finite-dimensional subspace V_n of complex polynomials of degree $< n$ is invariant under D; what is the Jordan canonical form of the restriction of D to this subspace?

7. Consider groups of order 70. Are they all abelian or solvable? Can you say anything regarding their normal subgroup structure?

Algebra, May 1978

1. Give an example of a nonabelian simple group. Do not prove your assertion.

2. Let G be a finite p-group acting linearly on a finite dimensional vector space over $\mathbb{Z}_p$. Prove G has a non-zero fixed point.

3. Describe the semisimple 4-dimensional algebras over the reals $\mathbb{R}$. (No proofs required.)

4. Describe the modules over the ring $M_n(F)$ of $n \times n$ matrices over a field F.

5. Is the ring $C[0,1]$ of all real-valued continuous functions on the interval $[0,1]$ Noetherian (i.e., does it satisfy the ascending chain condition on ideals)? Justify your assertion.

6. Give an example of a torsion free abelian group which is not free. Can you give an example which is finitely generated?

7. Find the inverse of the matrix
$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

8. (a) What is the Jordan canonical form of the matrix
$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

   (b) Give the eigenvalues, characteristic and minimum polynomials for this matrix.

9. Show that any two eigenvectors with distinct eigenvalues of the matrix
$$\begin{pmatrix} 1 & 9 & 7 & 8 \\ 9 & 0 & 0 & 0 \\ 7 & 0 & 1 & 0 \\ 8 & 0 & 0 & 0 \end{pmatrix}$$
   are orthogonal.

10. Give a polynomial whose splitting field is a field with 9 elements. Can this be done in a

12. Fill in the blank:

$$\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Z}_4 \cong \underline{\qquad\qquad}$$

$$\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Z} \cong \underline{\qquad\qquad}$$

$$\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Q} \cong \underline{\qquad\qquad}$$

$$\mathrm{Hom}(\mathbb{Z}_6, \mathbb{Z}_{14}) \cong \underline{\qquad\qquad}$$

13. Define "projective module." Is there a dual notion?

Algebra, September 1978

1. Prove that the set of rational 3×3 matrices which commute with the matrix

$$\begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & 4 \\ 0 & 1 & 2 \end{bmatrix}$$

is a field.

2. Let V be a 12-dimensional vector space over the field $GF(3)$. Let T be a linear transformation whose characteristic polynomial factors into linear factors over $GF(3)$. Find all possible Jordan normal forms given the table:

Transformation	**Rank**
T	10
T^2	9
T^3	9
$T-1$	12
$T-2$	9
$(T-2)^2$	7
$(T-2)^3$	6

3. A certain group of order 60 is known to have exactly four members of order 5. Explain why they, along with the identity, form a normal subgroup.

4. (a) Show that the Galois group over the rationals of every irreducible 5th degree polynomial contains an element of order 5.

   (b) Show that the Galois group over the rationals of x^4+1 does not contain an element of order 4.

   (c) Show that the Galois group over the rationals of x^4+x^3+1 contains an element of order 4.

5. Let M be a module over an integral domain A with quotient field K. Show that M is torsion free if and only if $0 \to M \to M \otimes_A \mathcal{K}$ is exact.

7. Let A be a simple Artinian ring, and let N be a minimal right ideal.

   (a) Viewing N as a right A-module, show that the ring $D = \mathrm{End}_A(N)$ of A-linear endomorphisms of N is a division ring.

   (b) Prove $AN = A$.

   (c) Let k be minimal such that there exist $m_1, \ldots, m_k$ in N and $a_1, \ldots, a_k$ in A with $1 = a_1 m_1 + \cdots + a_k m_k$. Prove that the map

$$\underbrace{N \oplus \cdots \oplus N}_{k-\text{copies}} \to A$$

   given by $(x_1, \ldots, x_k) \to a_1 x_1 + \cdots + a_k x_k$ is an isomorphism of right A-modules.

   (d) Deduce $A \cong \mathrm{End}_A(N^k) \simeq M_k(D)$, the algebra of $k \times k$ matrices over D. What famous theorem is this?

Algebra, May 1980

1. Describe all abelian groups of order 375. Be sure that you have at least listed each possibility up to isomorphism in some fashion.

2. A famous theorem of Hilbert states that $k[x_1, \ldots, x_n]$ is a Noetherian ring when k is a field. Prove in *detail* that every commutative k-algebra, A, which can be generated as a k-algebra by a finite number of elements is also Noetherian, that is, satisfies the ascending chain condition.

3. Give the eigenvalues of the following matrices. What are their Jordan normal forms?

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

4. Let $Q(X)$ be a quadratic form for $X = (x_1, x_2)$ in $\mathbb{R}^2$ given by

$$Q(X) = ax_1^2 + bx_1x_2 + cx_2^2.$$

Recall that the bilinear form $B(U, V)$ associated with a quadratic form $Q(X)$ is given by

$$B(U, V) = Q(U + V) - Q(U) - Q(V).$$

   (a) What is the associated (symmetric) bilinear form for $Q(X)$?

   (b) Show that the associated (symmetric) bilinear form for $Q(X)$ is non-degenerate if and only if $b^2 - 4ac \neq 0$.

5. Let A be a finite-dimensional algebra over the field, $\mathbb{C}$, of complex numbers.

   What can you say about A in the following cases?

   (a) A is simple.

   (b) A is semi-simple.

   (c) Let $T : V \to V$ be a linear transformation on the finite-dimensional vector space over $\mathbb{C}$. Let $A = \mathbb{C}[T]$ be the algebra of polynomials in T over $\mathbb{C}$. When is A a simple algebra?

   (d) When is the algebra of part (c) semi-simple and what can you say about T in this case?

Algebra, September 1980

1. Describe all abelian groups of order 80. Be sure that you have listed each possibility once and only once up to isomorphism.

2. A field is a trivial example of a principal ideal domain (P.I.D.). All abelian groups are modules for another well-known P.I.D., namely the ring _____. Give a third example of a P.I.D. Show that every homomorphic image of a P.I.D. is a principal ideal ring.

3. Suppose A is a 4×4 matrix with complex entries with $p(A) = 0$ for $p(t) = t^2 - 7t + 10$ and trace $A = 11$. Knowing trace $A = 11$, it is relatively easy to find all possible Jordan canonical forms for A. Find these forms and briefly explain your reasoning.

   What is the determinant of A?

4. Let V be a finite-dimensional vector space over a field k. The dual, V^*, of V is defined as the collection of all linear maps $V \to k$ (often called "linear functionals") with the vector space operations defined in the obvious way. If $v_1, \ldots, v_n$ is a basis for V, define $v_1^*, \ldots, v_n^*$ in V^* as the unique linear maps $V \to k$ satisfying

$$v_i^*(v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

   (a) Why, exactly, do there exist linear maps satisfying this condition?

   (b) Show that $v_1^*, \ldots, v_n^*$ is a basis for v^* (often called the "dual basis" associated with $v_1, \ldots, v_n$).

5. (a) Explain what it means to say that a sequence

$$0 \to U \to V \to W \to 0$$

   of vector spaces and linear maps is exact.

   What does it mean to say that the sequence

$$(*) \qquad 0 \to V_1 \to V_2 \to \cdots \to V_n \to 0$$

   of vector spaces and linear maps is exact?

   (b) If the sequence $(*)$ is exact and each V_i is of finite dimension, m_i, show that

Let $T : V \to V$ be a linear transformation on the finite-dimensional vector space, V, over $\mathbb{C}$. Let $A = \mathbb{C}[T]$ be the algebra of polynomials in T over $\mathbb{C}$. Under these hypotheses:

(c) When is A a simple algebra?

(d) When A is semi-simple and what can you infer about T in this case?

7. Let $F = Q(\sqrt{2}, \sqrt{3})$. It may be shown, and you may assume, that the Galois group is of order 4 and isomorphic to the "Klein 4-group" (the direct product of a cyclic group of order 2 with itself). Describe all the subfields of F and justify your description.

Algebra General Exam August 22, 1998

This is exam is worth 100 points. The number of points each part of a problem is worth is indicated in brackets. If you can't prove part of some problem, you can still use the result of that part in proving subsequent parts.

(1)[20] Let G be a finite group of order $3 \cdot 5 \cdot 17$.

(a)[5] Show that the Sylow 17-subgroup is normal.

(b)[5] *If there exists an element of order 15 in G,* show that the Sylow 3- and 5-subgroups are also normal. [Hint: show they are properly contained in their normalizers.]

(c)[5] If all Sylow subgroups of a finite group G are normal and abelian, show that G itself is abelian.

(d)[5] If G is a finite abelian group of order $p \cdot q \cdot r$ for distinct primes p, q, r, show that G is cyclic.

(2)[15] Let $GL_2(p)$ for a prime p denote the group of invertible 2×2 matrices over the finite field F_p of p elements.

(a)[5] Find the order n of the group $GL_2(p)$.

(b)[5] For λ in F_p, the find the order m of the subgroup

$$G_\lambda = \{A \in GL_2(p) \mid A \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} A^{-1} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}\}.$$

(c)[5] Find how many 2×2 matrices over F_p are similar to the matrix $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. [Hint: express it in terms of m and n.]

(3)[10] For an abelian group A, the *dual group* A^* is defined to be $Hom(A, U)$ where the *circle group* U is the multiplicative group of complex numbers of modulus 1 (the unit circle in the complex plane). Here $Hom(A, B)$ denotes the abelian group of homomorphisms of A into B (under $(f + g)(a) = f(a) + g(a)$); you may use the additivity property $Hom(A_1 \oplus A_2, B) \cong Hom(A_1, B) \oplus Hom(A_2, B)$ and the isomorphism property that if $A \cong A', B \cong B'$ then $Hom(A, B) \cong Hom(A', B')$.

(a)[5] Prove that Z_n^* is cyclic of order n.

(b)[5] Prove that A^* is isomorphic to A for *any* finite abelian group A.

(4)[10] Let a, b, c be distinct elements of an integral domain D. Show that there are *unique* elements x, y, z in D such that

$$\begin{aligned} x + y + z &= 0 \\ ax + by + cz &= 0 \\ a^2x + b^2y + c^2z &= 0 \end{aligned}.$$

for all elements a, b of R. Show that if D is a derivation, and in addition $D^2 = 0$ and R has no 2-torsion ($2a = 0$ implies $a = 0$), then the "exponential map" $Id + D$ is an *automorphism* of R.

(6)[15] Let V be an n-dimensional vector space over the complex numbers, and let T be a linear transformation from V to itself whose minimum polynomial $\mu(x)$ has degree 2.

(a)[5] Find all possible Jordan Canonical Forms for T. [Hint: consider the possible factorizations of $\mu(x)$ over K.]

(b)[5] Show that V is a direct sum of T-invariant subspaces, each of which has dimension less than or equal to 2.

(c)[5] Show that T has an eigenvalue λ such that the λ-eigenspace (the set of all eigenvectors for the eigenvalue λ, together with the zero vector) has dimension at least $n/2$.

(7)[10] Suppose that K is a finite Galois extension of the rational field Q which contains $\sqrt{3}$ and has cyclic Galois group $Gal(K/Q)$. Show that $L = Q(\sqrt{3})$ is the only quadratic extension of Q contained in K.

(8)[10] (a)[5] If F denotes a field and Z the ring of integers, decide which of the following rings are PIDs and which are UFDs (no proofs are necessary):

$$F,\ Z,\ Z[x],\ F[x, y],\ F[[x]]\ \text{(formal power series)}.$$

(b)[5] The *Krull dimension* of a commutative ring R is the longest chain of prime ideals properly contained in R, i.e. the largest integer n such that there exists a chain $P_0 < P_1 < \ldots < P_n < R$ ($P_0 = 0$ allowed if prime) of *prime ideals* P_i in R. If R is a PID, find its Krull dimension.

Algebra General Exam August 21, 1999

This is exam is worth 100 points. The number of points each part of a problem is worth is indicated in brackets. If you can't prove part of some problem, you can still use the result of that part in proving subsequent parts.

(1)[10] Let P be a p-Sylow subgroup of a finite group G for some prime p dividing the group order. We know by Sylow theory that the index of the normalizer of P is congruent to 1 modulo p,

$$[G : N_G(P)] \equiv 1 \pmod{p}.$$

Show that the same holds for any larger subgroup M: if $G \supseteq M \supseteq N_G(P)$ then

$$[G : M] \equiv 1 \pmod{p}.$$

[Hint: show $N_M(P) = N_G(P)$.]

(2)[20] (a)[5] Show that any finite group G has a faithful action on some set S of cardinality $|S| = |G|$.

From now on (in parts b,c) assume that G is a finite p-group for a prime p, having the property that it has a *unique* subgroup G_p of order p. [The quaternion group is such a group, with $p = 2$ and $G_2 = \{1, -1\}$.]

(b)[5] Show that G_p is invariant under all endomorphisms of G, $f(G_p) \subseteq G_p$ for all homomorphisms $f : G \to G$.

(c)[10] Show that G_p "needs room" in order to act: whenever G acts on a finite set S of size $|S| < |G|$, the subgroup G_p acts trivially. Conclude that G can only act faithfully on sets of size $\geq |G|$.

(3)[10] The *exponent* e of a group G is defined as the smallest positive integer k such that $x^k = 1$ for all $x \in G$; for an abelian group, in additive notation this is the smallest k such that $kx = 0$ for all elements. If $n_1, n_2, \ldots, n_r$ are the invariant factors of a finite abelian group A (so $n_r | n_{r-1} | \ldots | n_2 | n_1$), *prove* that A has exponent $e = n_1$, and has an element of order precisely e. Conclude that A has an element of order m iff m divides the largest invariant factor n_1.

(4)[10] If R is a (commutative, unital) integral domain, find all R-linear automorphisms of the polynomial ring $R[x]$ (all ring automorphisms φ with $\varphi(a) = a$ for all constant polynomials $a \in R$). [If you can't do the general case, do the case when $R = F$ is a field.]

(5)[10] Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ ($a_0 \neq 0$) be a complex polynomial of degree $n > 1$, and f' its derivative. Let $\alpha_1, \ldots \alpha_n$ be the n roots of f and $\alpha'_1, \ldots, \alpha'_{n-1}$ the $n-1$ roots of the derivative (listing each root as many times as its multiplicity). Show that the *average* of the roots $\alpha_1, \ldots \alpha_n$ of f equals the *average* of the roots $\alpha'_1, \ldots, \alpha'_{n-1}$ of f'. [Hint: Use the relations between the coefficients of a polynomial and the roots of that polynomial.]

(6)[10] Describe (in terms of Jordan form) all 2×2 complex matrices which are similar to their square. [Hint: there are more matrices, Horatio, than are dreamt of in your philosophy!]

(7)[10] (a)[5] Show that the ring of $2n \times 2n$ matrices $M_{2n}(F)$ over a field F for $n \geq 1$ is "algebraically closed" with respect to polynomials of degree 2, in the sense that every polynomial $p(x) = x^2 + \alpha x + \beta \in F[x]$ of degree 2 has a "root" $A \in M_{2n}(F)$ (in the sense that $p(A)$ is the zero matrix). Can you generalize this to polynomials of degree d?

(b)[5] How many real 2×2 matrices $A \in M_2(\mathbb{R})$ are roots of the polynomial $p(x) = x^2 + 1$?

(8)[10] If F is a *finite field* show that every element $\alpha \in F$ is the sum $\alpha = \beta_1^2 + \beta_2^2$ of two squares (for some $\beta_1, \beta_2 \in F$).

(9)[10] If p is a prime number congruent to 1 mod 8, *show* that 2 is a "quadratic residue" mod p, i.e. there is an integer a such that $a^2 \equiv 2$ modulo p. [Hint: show there is an $\varepsilon \in \mathbb{Z}_p$ with $\varepsilon^4 = -1$, and $\alpha^2 = 2$ for $\alpha = \varepsilon + \varepsilon^{-1}$.]

PROOFS

Proof (1): (1) $N_M(P) = M \cap N_G(P)$ (always) $= N_G(P)$ (when $M \supseteq N_G(P)$). (2) Using Sylow on both G and M (noting that P remains a p-Sylow subgroup of M) shows the indexes of the normalizers is congruent to 1, so $[G : N_G(P)] \equiv 1, [M : N_G(P)] = [M : N_M(P)] \equiv 1,\ 1 \equiv [G : N_G(P)] = [G : M][M : N_G(P)] \equiv [G : M]1 = [G : M]$.

Proof (2a): Left-regular representation.

Proof (2b): G_p is in fact the set of all elements of order 1 or p [any element g of order p generates a cyclic subgroup of order p, which by uniqueness must be G_p, therefore $g \in G_p$], hence is invariant under any homomorphism.

Proof (2c): For any $s \in S$ we have $|G| > |S| \geq G \cdot s = [G : Stab(s)]$ (orbit size formula) $= |G|/|Stab(s)|$ so $|Stab(s)| > 1$. Thus $|Stab(s)|$ is a power of p, in particular (by Cauchy) has an element of order p, hence a cyclic subgroup of order p, which by uniqueness must be $G_p : G_p \subseteq Stab(s)$. Thus G_p fixes all points s, thus acts trivially on S.

Proof (3): In $A = \bigoplus Z_{n_i}$, any $x = \sum x_i$ has $x^{n_1} = \sum x_i^{n_1} = 1$ since n_1 is a multiple of n_i, and this is the smallest such power since the generator of Z_{n_1} has order exactly n_1. If m divides n_1 then there exists $Z_m \subseteq Z_{n_1} \subseteq A$. Conversely, if A has an element x of order m then m divides the exponent n_1 (by the above).

Proof (4) The automorphism are precisely all "linear" transformation $\varphi_{a,b}(f(x)) = f(ax + b)$ for invertible a and arbitrary b in R, with inverse $\varphi_{a^{-1},-a^{-1}b}$. Indeed, if $\varphi(x) = f(x), \varphi^{-1}(x) = g(x)$, for f, g of degrees n, m, then $x = \varphi(\varphi^{-1}(x)) = \varphi(g(x)) = g(f(x))$ shows $1 = mn$ (over a domain the degree of the product is $n + m$ and the degree of the composite is nm), so $n = m = 1, f(x) = ax+b, g(x) = cx+d, x = c(ax+b)+d = (ca)x+(cb+d)$ implies $ca = 1$ (so a is invertible with inverse c) and $cb + d = 0$ (so $d = -cb$).

Proof (5): $\frac{1}{n}\sum_{i=1}^{n} \alpha_i = -\frac{1}{n}(\frac{a_{n-1}}{a_n}),\ \frac{1}{n-1}\sum_{i=1}^{n-1} \alpha_i' = -\frac{1}{n-1}(\frac{(n-1)a_{n-1}}{na_n})$.

Proof (6) (1) if the distinct diagonal entries of the Jordan form A are λ, μ then A^2 has diagonal entries λ^2, μ^2 then we either have (1a) $\lambda = \lambda^2, \mu = \mu^2$, so $\lambda, \mu = 0, 1$ and by distinctness $\lambda = 1, \mu = 0$ and we have an idempotent $A \sim \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, or we have (1b) $\lambda = \mu^2, \mu = \lambda^2$, so $\lambda^4 = \lambda \neq 0, 1, \lambda^3 = 1, \lambda = \zeta$ is a primitive cube root of unity and $\mu = \lambda^2 = \lambda^{-1}$, and we have $A \sim \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$. (2) If $A = \lambda I$ then $A^2 = \lambda^2 I$ and we must have $\lambda = \lambda^2$, so again we have idempotents $A = I, 0$. (3) If $A \sim \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ is a 2×2 Jordan block, then $A^2 \sim \begin{pmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda^2 \end{pmatrix}$, so again $\lambda = \lambda^2, \lambda = 1, 0$; but we can't have $\lambda = 0$ (A would be nilpotent of index 2, $A^2 = 0$ nilpotent of index 1, so not similar), hence $A \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $A^2 \sim \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \sim A$.

Proof (7a) Any $p(x)$ has root A consisting of n blocks B_2 strung together down the diagonal (hence the need for even size $2n$), where B_2 is the 2×2 *companion matrix of* $p(x)$, namely $\begin{pmatrix} -\alpha & 1 \\ -\beta & 0 \end{pmatrix}$, and Z_{n-2} the $(n-2) \times (n-2)$ zero matrix. More generally, any polynomial $p(x) = x^d + \alpha_{d-1}x^{d-1} + \ldots + \alpha_1 x + \alpha_0$ has root obtained by duplicating its $d \times d$ companion matrix $n \geq 1$ times to obtain a $dn \times dn$ matrix.

Proof (7b): There are infinitely many distinct conjugates of any solution A, and there is only one Jordan form for a real matrix having minimum polynomial dividing $x^2 + 1$, namely $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ with rational canonical

Proof (9): $\mathbb{Z}_p^\times$ is a cyclic group of order $p-1$ divisible by 8, so it has a unique cyclic subgroup $<\varepsilon>$ of order 8; ε^4 is not 1, yet it is a square root of unity in the field, so it must be -1. The $(\varepsilon+\varepsilon^{-1})^2 = \varepsilon^2 + 2 + \varepsilon^{-2} = 2$ because $\varepsilon^{-2}, \varepsilon^2$ are negatives of each other: both have the same square $(-1)^{-1} = -1$, yet they are not equal (since $\varepsilon^4 \neq 1$), so their quotient squares to 1 but isn't one, and must be the only other square root of unity, namely -1.

General Exam - Algebra

August 14, 2000

1. Let V be a vector space over the field of reals $\mathbb{R}$. Show that V cannot be presented as the union of three proper subspaces.
2. Let K be an arbitrary field, G be a finite group of order $n > 1$. Show that the group algebra $K[G]$ has zero divisors. Does this result remain true for infinite groups?
3. Prove or disprove: A commutative local ring has only one nonzero prime ideal (by definition, a commutative ring is called *local* if it has only one *maximal* ideal).
4. For a field K, we denote by $K(x)$ the field of rational functions in one variable x over K. Prove or disprove: $\mathbb{C}(x)$ is the algebraic closure of $\mathbb{R}(x)$.
5. Let K be the splitting field of the polynomial $f(x) = x^{13} - 1$ over $\mathbf{F}_5$ (the field of 5 elements). Determine the Galois group $Gal(K/\mathbf{F}_5)$.
6. Let a and b be positive relatively prime integers. Show that any integer $N > ab$ can be written in the form $N = ax + by$ where x, y are integers ≥ 0.
7. (a) Let G be a finite group of order $p^\alpha m$ where p is a prime relatively prime to m, and let G_p denote the set of elements of G whose order is p^i for some $i > 0$. Show that

$$| G_p | \leq [G : N](p^\alpha - 1)$$

where N is the normalizer of some Sylow p-subgroup, with equality holding iff any two distinct Sylow p-subgroups have trivial intersection.

(b) Let G be a finite group of order $p^\alpha q^\beta$ for distinct primes p, q. Assume that G does not have elements of mixed order (i.e. the order of any element is either p^i or q^j) and has a normal Sylow q-subgroup. Show that

$$| G_p | = q^\beta(p^\alpha - 1).$$

Using (a), conclude that in this case any two distinct Sylow p-subgroups intersect trivially.

(over, please)

8. Determine all possibilities for the Jordan canonical form of a matrix $A \in GL_2(\mathbb{C})$ given that A is conjugate to ${}^tA^{-1}$ where ^{t} denotes the operation of taking the transpose of a matrix.

9. Let R denote the set of complex numbers of the form $a+b\sqrt{-6}$ with $a, b \in \mathbb{Z}$.

   (i) Show that R is a subring of $\mathbb{C}$.

   (ii) Let $\mathfrak{a}$ be the ideal of R generated by 5 and $2+\sqrt{-6}$. Show that $\mathfrak{a}$ is proper (i.e. $\mathfrak{a} \neq R$). (*Hint.* Use the conjugate $2-\sqrt{-6}$.)

   (iii) Show that the ideal $\mathfrak{a}$ is prime, while the ideal $\mathfrak{b} \subset R$ generated by 5 alone is not prime. (*Hint.* For the first part, try to identify the quotient ring $R/\mathfrak{a}$.)

10. Let R be a unital commutative ring. From the usual theory of determinants for matrices over R, we know that if $M \simeq R^n$ is a <u>free</u> module we can uniquely define the determinant $\det(T)$ to any $T \in \mathrm{End}_R(M)$. Suppose M is only a <u>direct summand</u> of a free module, $M \oplus M' \simeq R^n$ for some (finite) n. Define $\tilde{T} = T \oplus 1_{M'} \in \mathrm{End}_R(M \oplus M')$ and set

$$\det_{M,M'}(T) := \det(\tilde{T}).$$

Show that this is independent of the complement chosen: if also $M \oplus M'' \simeq R^m$ and $\hat{T} = T \oplus 1_{M''}$, then $\det(\hat{T}) = \det(\tilde{T})$ as elements of R. (*Hint.* Show that there are two

$$S_1, S_2 \in \mathrm{End}_R(M \oplus M' \oplus M \oplus M'') \simeq \mathrm{End}_R(R^{n+m})$$

with $\det(S_1) = \det_{M,M'}(T)$, $\det(S_2) = \det_{M,M''}(T)$, and $S_2 = PS_1P^{-1}$ for an invertible $P \in \mathrm{End}_R(M \oplus M' \oplus M \oplus M'')$.) Conclude that there is a well-defined determinant for endomorphisms of such M's, which agrees with the usual determinant for free modules M.

Algebra, April 1977

1. Let C be the field of complex numbers, and let A be an $n \times n$ matrix over C. As usual, we define $e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!} = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots$, where the convergence of the series is that of C^{n^2}.

   (a) Use the Jordan canonical form to show that $\det e^A = e^{TrA}$.

   (b) If $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, what is e^A?

2. Let k be a field of q elements where q is finite.

   (a) Show that $q = p^n$ is a power of a prime.

   (b) Show that k is the splitting field of the equation $x^q - x = 0$ and thus is the unique field of q elements.

   (c) The multiplicative group k^* of non-zero elements of k satisfy the equation $x^{q-1} - 1 = 0$. Why does this imply that k^* is a *cyclic* group of order $q - 1$?

3. Use the fundamental theorem for abelian groups to show that in the ring of integers mod p^n, for p an odd prime, the multiplicative group of integers relatively prime to p has a subgroup of order p if $n > 1$.

4. Let R be a commutative ring with 1 and let M be a maximal ideal in R. Show that R/M is a field.

   (a) Show that if R is a Euclidean Integral Domain then every ideal generated by an irreducible element is maximal.

   (b) Let k be a field and $R = k[x]$ the polynomial ring in one variable over k. If $p(x) = p$ is an irreducible polynomial in $k[x]$ use 4. and (a) to show that there is a finite extension K of k in which $p(x)$ has a root.

   (c) If $k = Q$ is the rational field and $p(x) = x^2 + x + 1$ show that $p(x)$ is indeed irreducible over Q. What is the field generated in (b) for this example?

5. Let $G = S_n$ be the symmetric group on n letters.

   (a) Show that the alternating group A_n on n letters is a normal subgroup of S_n.

   (b) Show that A_n is generated by the three-cycles $(1, 2, i)$,$i = 3, 4, \ldots, n$.

   (c) Show that if H is a normal subgroup of A_n for $n \geq 3$ and H contains a 3-cycle, then $H = A_n$.

6. Let $k = Q$ be the rational field and let $f(x) = x^3 + 5$.

   (a) Show that $f(x)$ is irreducible over Q.

   (b) Use Galois theory to show that the Galois group of $f(x)$ cannot be of order 3.

   (c) Find the Galois group of $f(x)$.

(d) Is the equation $f(x)$ solvable by radical? Give reasons for your answer.

7. Let A be a normal ($A^*A = AA^*$) $n \times n$ complex matrix. Show that there is a polynomial $f(x)$ with complex coefficients such that $A^* = f(A)$. Thus any $n \times n$ matrix B which commutes with A also commutes with A^*. (Assume the spectral theorem for A.)

8. If A and B are algebras over a field k define their tensor product $C = A \otimes_k B$ and show that C is an algebra over k.

   (a) Let A and B each have units and let $Z(A) = Z_1$, $Z(B) = Z_2$, and $Z(C) = Z$ designate the centers of A, B, and C respectively. Show that $Z = Z_1 \otimes Z_2$.

Algebra, November 1977

1. How many non-isomorphic fields are there with exactly 3 elements? Exactly 6 elements? Exactly 9 elements?

2. Describe the following tensor products of modules in more explicit form. (Z = integers).

   (i) $Z_2 \otimes_{Z_4} Z_4$

   (ii) $Z_2 \otimes_Z Z_3$

   (iii) $Z_2 \otimes_{Z_3} Z$

3. Give an example of an *inseparable* extension of degree 7 over Q (the rationals).

4. Define "finite" and "algebraic" extensions of fields. Does algebraic imply finite? Does finite imply algebraic? Prove or give counterexample.

5. Give an example of a non-Noetherian commutative ring.

6. Find all eigenvectors and eigenvalues of the linear operator $D = \frac{d}{dx}$ (differentiation) on the space $V = C^\infty(R)$ of infinitely differentiable complex-valued functions on the real line R. The finite-dimensional subspace V_n of complex polynomials of degree $< n$ is invariant under D; what is the Jordan canonical form of the restriction of D to this subspace?

7. Consider groups of order 70. Are they all abelian or solvable? Can you say anything regarding their normal subgroup structure?

Algebra, May 1978

1. Give an example of a nonabelian simple group. Do not prove your assertion.

2. Let G be a finite p-group acting linearly on a finite dimensional vector space over $\mathbb{Z}_p$. Prove G has a non-zero fixed point.

3. Describe the semisimple 4-dimensional algebras over the reals $\mathbb{R}$. (No proofs required.)

4. Describe the modules over the ring $M_n(F)$ of $n \times n$ matrices over a field F.

5. Is the ring $C[0,1]$ of all real-valued continuous functions on the interval $[0,1]$ Noetherian (i.e., does it satisfy the ascending chain condition on ideals)? Justify your assertion.

6. Give an example of a torsion free abelian group which is not free. Can you give an example which is finitely generated?

7. Find the inverse of the matrix
$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

8. (a) What is the Jordan canonical form of the matrix
$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

   (b) Give the eigenvalues, characteristic and minimum polynomials for this matrix.

9. Show that any two eigenvectors with distinct eigenvalues of the matrix
$$\begin{pmatrix} 1 & 9 & 7 & 8 \\ 9 & 0 & 0 & 0 \\ 7 & 0 & 1 & 0 \\ 8 & 0 & 0 & 0 \end{pmatrix}$$
   are orthogonal.

10. Give a polynomial whose splitting field is a field with 9 elements. Can this be done in a similar way for a field of 18 elements?

11. Say what you can about the intermediate subfields of a Galois extension E/F with Galois group the symmetric group S_3.

12. Fill in the blank:

$$\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Z}_4 \cong \underline{\qquad\qquad}$$

$$\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Z} \cong \underline{\qquad\qquad}$$

$$\mathbb{Z}_6 \otimes_{\mathbb{Z}} \mathbb{Q} \cong \underline{\qquad\qquad}$$

$$\mathrm{Hom}(\mathbb{Z}_6, \mathbb{Z}_{14}) \cong \underline{\qquad\qquad}$$

13. Define "projective module." Is there a dual notion?

Algebra, September 1978

1. Prove that the set of rational 3×3 matrices which commute with the matrix

$$\begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & 4 \\ 0 & 1 & 2 \end{bmatrix}$$

is a field.

2. Let V be a 12-dimensional vector space over the field $GF(3)$. Let T be a linear transformation whose characteristic polynomial factors into linear factors over $GF(3)$. Find all possible Jordan normal forms given the table:

Transformation	**Rank**
T	10
T^2	9
T^3	9
$T-1$	12
$T-2$	9
$(T-2)^2$	7
$(T-2)^3$	6

3. A certain group of order 60 is known to have exactly four members of order 5. Explain why they, along with the identity, form a normal subgroup.

4. (a) Show that the Galois group over the rationals of every irreducible 5th degree polynomial contains an element of order 5.

   (b) Show that the Galois group over the rationals of x^4+1 does not contain an element of order 4.

   (c) Show that the Galois group over the rationals of x^4+x^3+1 contains an element of order 4.

5. Let M be a module over an integral domain A with quotient field K. Show that M is torsion free if and only if $0 \to M \to M \otimes_A \mathcal{K}$ is exact.

6. A local ring is defined to be a commutative ring with unit having a unique maximal ideal.

   (a) Prove a commutative ring, R, is local if and only if the non-units form an ideal.

   (b) A domain, V, is called a valuation domain if for $a, b \in V$ either a divides b or b divides a. Show that a valuation domain is a local ring.

   (c) Prove that a local ring has no idempotents (other than 1).

7. Let A be a simple Artinian ring, and let N be a minimal right ideal.

   (a) Viewing N as a right A-module, show that the ring $D = \mathrm{End}_A(N)$ of A-linear endomorphisms of N is a division ring.

   (b) Prove $AN = A$.

   (c) Let k be minimal such that there exist $m_1, \ldots, m_k$ in N and $a_1, \ldots, a_k$ in A with $1 = a_1 m_1 + \cdots + a_k m_k$. Prove that the map

$$\underbrace{N \oplus \cdots \oplus N}_{k-\text{copies}} \to A$$

   given by $(x_1, \ldots, x_k) \to a_1 x_1 + \cdots + a_k x_k$ is an isomorphism of right A-modules.

   (d) Deduce $A \cong \mathrm{End}_A(N^k) \simeq M_k(D)$, the algebra of $k \times k$ matrices over D. What famous theorem is this?

Algebra, May 1980

1. Describe all abelian groups of order 375. Be sure that you have at least listed each possibility up to isomorphism in some fashion.

2. A famous theorem of Hilbert states that $k[x_1, \ldots, x_n]$ is a Noetherian ring when k is a field. Prove in *detail* that every commutative k-algebra, A, which can be generated as a k-algebra by a finite number of elements is also Noetherian, that is, satisfies the ascending chain condition.

3. Give the eigenvalues of the following matrices. What are their Jordan normal forms?

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

4. Let $Q(X)$ be a quadratic form for $X = (x_1, x_2)$ in $\mathbb{R}^2$ given by

$$Q(X) = ax_1^2 + bx_1x_2 + cx_2^2.$$

   Recall that the bilinear form $B(U, V)$ associated with a quadratic form $Q(X)$ is given by

$$B(U, V) = Q(U + V) - Q(U) - Q(V).$$

   (a) What is the associated (symmetric) bilinear form for $Q(X)$?

   (b) Show that the associated (symmetric) bilinear form for $Q(X)$ is non-degenerate if and only if $b^2 - 4ac \neq 0$.

5. Let A be a finite-dimensional algebra over the field, $\mathbb{C}$, of complex numbers.

   What can you say about A in the following cases?

   (a) A is simple.

   (b) A is semi-simple.

   (c) Let $T : V \to V$ be a linear transformation on the finite-dimensional vector space over $\mathbb{C}$. Let $A = \mathbb{C}[T]$ be the algebra of polynomials in T over $\mathbb{C}$. When is A a simple algebra?

   (d) When is the algebra of part (c) semi-simple and what can you say about T in this case?

   Note: In parts (c) and (d), your answer should specify conditions on the transformation T.

6. Let $F = Q(\zeta)$ where ζ is a primitive n^{th} root of 1. Let a be a non-zero element of F which is not an n^{th} root in F. Show that the galois group of the field $K = F\left(\sqrt[n]{a}\right)$ over F is abelian.

Algebra, September 1980

1. Describe all abelian groups of order 80. Be sure that you have listed each possibility once and only once up to isomorphism.

2. A field is a trivial example of a principal ideal domain (P.I.D.). All abelian groups are modules for another well-known P.I.D., namely the ring _____. Give a third example of a P.I.D. Show that every homomorphic image of a P.I.D. is a principal ideal ring.

3. Suppose A is a 4×4 matrix with complex entries with $p(A) = 0$ for $p(t) = t^2 - 7t + 10$ and trace $A = 11$. Knowing trace $A = 11$, it is relatively easy to find all possible Jordan canonical forms for A. Find these forms and briefly explain your reasoning.

   What is the determinant of A?

4. Let V be a finite-dimensional vector space over a field k. The dual, V^*, of V is defined as the collection of all linear maps $V \to k$ (often called "linear functionals") with the vector space operations defined in the obvious way. If $v_1, \ldots, v_n$ is a basis for V, define $v_1^*, \ldots, v_n^*$ in V^* as the unique linear maps $V \to k$ satisfying

$$v_i^*(v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

   (a) Why, exactly, do there exist linear maps satisfying this condition?

   (b) Show that $v_1^*, \ldots, v_n^*$ is a basis for v^* (often called the "dual basis" associated with $v_1, \ldots, v_n$).

5. (a) Explain what it means to say that a sequence

$$0 \to U \to V \to W \to 0$$

   of vector spaces and linear maps is exact.

   What does it mean to say that the sequence

$$(*) \qquad 0 \to V_1 \to V_2 \to \cdots \to V_n \to 0$$

   of vector spaces and linear maps is exact?

   (b) If the sequence $(*)$ is exact and each V_i is of finite dimension, m_i, show that

$$m_1 - m_2 + m_3 - \cdots + (-1)^{n+1} m_n = 0.$$

6. Let A be a finite-dimensional algebra over the field $\mathbb{C}$ of complex numbers. What can you say about A in the following cases?

   (a) A is simple.

   (b) A is semi-simple.

Let $T : V \to V$ be a linear transformation on the finite-dimensional vector space, V, over $\mathbb{C}$. Let $A = \mathbb{C}[T]$ be the algebra of polynomials in T over $\mathbb{C}$. Under these hypotheses:

(c) When is A a simple algebra?

(d) When A is semi-simple and what can you infer about T in this case?

7. Let $F = Q(\sqrt{2}, \sqrt{3})$. It may be shown, and you may assume, that the Galois group is of order 4 and isomorphic to the "Klein 4-group" (the direct product of a cyclic group of order 2 with itself). Describe all the subfields of F and justify your description.

ALGEBRA GENERAL EXAMINATION

January 17, 1998

Question 1 (a) What can you say about groups G of the following orders $|G|$? (Give reasons, making free use of any theorems you know.)

(1) $|G| = 2^4 + 1 : G \cong ?$

(2) $|G| = 2^3 + 1 : G \cong ?$

(b) What can you say about *simple* groups G of the following orders $|G|$? (Again, explain your answer.)

(1) $|G| = 2^m + 1 : G \cong ?$

(2) $|G| = 2.3.5 : G \cong ?$

(3) $|G| = 2^2.3.5 : G \cong ?$

All your answers should be quite short.

Question 2 (a) How many non-isomorphic abelian groups are there of order 360?

(b) Take the free abelian group on generators x, y and z. Divide it by the relations

$$\begin{array}{rcrcrcl} 2x & + & 4y & + & 5z & = & 0 \\ 6x & + & 8y & + & 10z & = & 0 \\ 8x & + & 12y & + & 20z & = & 0 \end{array}$$

Write the resulting group as a direct sum of cyclic groups.

Question 3 Let R be a principal ideal domain. Suppose a and b are two non–zero elements in R. Show that they have a least common multiple. That means the following. We adopt the notation that $a \mid m$ means "a divides m". You need to show that there exists an element $m \in R$, so that

$$a \mid m \text{ and } b \mid m.$$

If $a \mid x$ and $b \mid x$, then $m \mid x$.

Question 4 Let M be a module over a ring. A *section* $A : B$ of M is a pair of submodules A, B of M with $B \subseteq A$; a *trivial section* is where $B = A$. A submodule C of M *covers* a section $A : B$ if $(A \cap C) + B = A$, and *avoids* $A : B$ if $A \cap C \subseteq B$.

(a) Show that C covers $A : B$ if and only if $A \subseteq B + C$, and avoids $A : B$ if and only if $A \cap (B + C) = B$.

(b) Show that every C simultaneously covers and avoids any trivial section, that any C with $C \supseteq A$ covers $A : B$, and any C with $C \subseteq B$ avoids $A : B$.

(c) Give an example of a Z-module M and a submodule C that covers one nontrivial section $A : B$ and avoids another nontrivial section $A' : B'$ for which the two quotients A/B and A'/B' are isomorphic.

Question 5 (a) Find the Galois group of the polynomial

$$x^5 + 5x^3 - 20x + 10$$

over the rational numbers.

(b) The Galois group G over F of a polynomial $f(x) \in F[x]$ of degree 4 is known to contain a subgroup isomorphic to the dihedral group D_4.

(1) Show that $f(x)$ is irreducible.

(2) If some root r_i of $f(x)$ lies in the subfield $F(r_j, r_k)$ generated by two other roots, show $F(r_j, r_k)$ is a splitting field for $f(x)$ and that $G = D_4$.

(3) Show that no root r_i of $f(x)$ is a *linear combination* of two other roots r_j, r_k.

Question 6 The finite field $GF(32)$ of 32 elements can be constructed as the extension $GF(2)(\theta)$, where θ is a root of the polynomial $x^5 + x^2 + 1$ in $GF(2)[x]$. Find the minimal polynomial of θ^3 over $GF(2)$.

Question 7 If the $n \times n$ real matrix P is the transition matrix for a regular Markov chain, then its powers converge to a matrix $T = \lim_{k\to\infty} P^k$ of the form $\begin{bmatrix} t_1 & t_1 & \dots & t_1 \\ \dots & \dots & \dots & \dots \\ t_n & t_n & \dots & t_n \end{bmatrix}$ all of whose columns are the same probability vector $\mathbf{t}$ (it's entries t_i are all nonnegative and sum to 1).

(a) What is the Jordan canonical form of the limit T?

(b) What are the possible complex eigenvalues of the original P?

(c) What are the possible Jordan canonical forms of P?

If you cannot do the general case, do at least the 2×2 case.

Algebra General Exam August 22, 1998

This is exam is worth 100 points. The number of points each part of a problem is worth is indicated in brackets. If you can't prove part of some problem, you can still use the result of that part in proving subsequent parts.

(1)[20] Let G be a finite group of order $3 \cdot 5 \cdot 17$.

(a)[5] Show that the Sylow 17-subgroup is normal.

(b)[5] *If there exists an element of order 15 in G,* show that the Sylow 3- and 5-subgroups are also normal. [Hint: show they are properly contained in their normalizers.]

(c)[5] If all Sylow subgroups of a finite group G are normal and abelian, show that G itself is abelian.

(d)[5] If G is a finite abelian group of order $p \cdot q \cdot r$ for distinct primes p, q, r, show that G is cyclic.

(2)[15] Let $GL_2(p)$ for a prime p denote the group of invertible 2×2 matrices over the finite field F_p of p elements.

(a)[5] Find the order n of the group $GL_2(p)$.

(b)[5] For λ in F_p, the find the order m of the subgroup

$$G_\lambda = \{A \in GL_2(p) \mid A \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} A^{-1} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}\}.$$

(c)[5] Find how many 2×2 matrices over F_p are similar to the matrix $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. [Hint: express it in terms of m and n.]

(3)[10] For an abelian group A, the *dual group* A^* is defined to be $Hom(A, U)$ where the *circle group* U is the multiplicative group of complex numbers of modulus 1 (the unit circle in the complex plane). Here $Hom(A, B)$ denotes the abelian group of homomorphisms of A into B (under $(f+g)(a) = f(a)+g(a)$); you may use the additivity property $Hom(A_1 \oplus A_2, B) \cong Hom(A_1, B) \oplus Hom(A_2, B)$ and the isomorphism property that if $A \cong A', B \cong B'$ then $Hom(A, B) \cong Hom(A', B')$.

(a)[5] Prove that Z_n^* is cyclic of order n.

(b)[5] Prove that A^* is isomorphic to A for *any* finite abelian group A.

(4)[10] Let a, b, c be distinct elements of an integral domain D. Show that there are *unique* elements x, y, z in D such that

$$\begin{aligned} x + y + z &= 0 \\ ax + by + cz &= 0 \\ a^2x + b^2y + c^2z &= 0 \end{aligned} .$$

(5)[10] A *derivation* D of a ring R is a map of R into itself such that

$$\begin{aligned} D(a+b) &= D(a)+D(b) \\ D(ab) &= D(a)b + aD(b) \end{aligned}$$

for all elements a, b of R. Show that if D is a derivation, and in addition $D^2 = 0$ and R has no 2-torsion ($2a = 0$ implies $a = 0$), then the "exponential map" $Id + D$ is an *automorphism* of R.

(6)[15] Let V be an n-dimensional vector space over the complex numbers, and let T be a linear transformation from V to itself whose minimum polynomial $\mu(x)$ has degree 2.

(a)[5] Find all possible Jordan Canonical Forms for T. [Hint: consider the possible factorizations of $\mu(x)$ over K.]

(b)[5] Show that V is a direct sum of T-invariant subspaces, each of which has dimension less than or equal to 2.

(c)[5] Show that T has an eigenvalue λ such that the λ-eigenspace (the set of all eigenvectors for the eigenvalue λ, together with the zero vector) has dimension at least $n/2$.

(7)[10] Suppose that K is a finite Galois extension of the rational field Q which contains $\sqrt{3}$ and has cyclic Galois group $Gal(K/Q)$. Show that $L = Q(\sqrt{3})$ is the only quadratic extension of Q contained in K.

(8)[10] (a)[5] If F denotes a field and Z the ring of integers, decide which of the following rings are PIDs and which are UFDs (no proofs are necessary):

$$F,\ Z,\ Z[x],\ F[x,y],\ F[[x]]\ \text{(formal power series)}.$$

(b)[5] The *Krull dimension* of a commutative ring R is the longest chain of prime ideals properly contained in R, i.e. the largest integer n such that there exists a chain $P_0 < P_1 < \ldots < P_n < R$ ($P_0 = 0$ allowed if prime) of *prime ideals* P_i in R. If R is a PID, find its Krull dimension.

Algebra General Exam August 21, 1999

This is exam is worth 100 points. The number of points each part of a problem is worth is indicated in brackets. If you can't prove part of some problem, you can still use the result of that part in proving subsequent parts.

(1)[10] Let P be a p-Sylow subgroup of a finite group G for some prime p dividing the group order. We know by Sylow theory that the index of the normalizer of P is congruent to 1 modulo p,

$$[G : N_G(P)] \equiv 1 \pmod{p}.$$

Show that the same holds for any larger subgroup M: if $G \supseteq M \supseteq N_G(P)$ then

$$[G : M] \equiv 1 \pmod{p}.$$

[Hint: show $N_M(P) = N_G(P)$.]

(2)[20] (a)[5] Show that any finite group G has a faithful action on some set S of cardinality $|S| = |G|$.

From now on (in parts b,c) assume that G is a finite p-group for a prime p, having the property that it has a *unique* subgroup G_p of order p. [The quaternion group is such a group, with $p = 2$ and $G_2 = \{1, -1\}$.]

(b)[5] Show that G_p is invariant under all endomorphisms of G, $f(G_p) \subseteq G_p$ for all homomorphisms $f : G \to G$.

(c)[10] Show that G_p "needs room" in order to act: whenever G acts on a finite set S of size $|S| < |G|$, the subgroup G_p acts trivially. Conclude that G can only act faithfully on sets of size $\geq |G|$.

(3)[10] The *exponent* e of a group G is defined as the smallest positive integer k such that $x^k = 1$ for all $x \in G$; for an abelian group, in additive notation this is the smallest k such that $kx = 0$ for all elements. If $n_1, n_2, \ldots, n_r$ are the invariant factors of a finite abelian group A (so $n_r | n_{r-1} | \ldots | n_2 | n_1$), *prove* that A has exponent $e = n_1$, and has an element of order precisely e. Conclude that A has an element of order m iff m divides the largest invariant factor n_1.

(4)[10] If R is a (commutative, unital) integral domain, find all R-linear automorphisms of the polynomial ring $R[x]$ (all ring automorphisms φ with $\varphi(a) = a$ for all constant polynomials $a \in R$). [If you can't do the general case, do the case when $R = F$ is a field.]

(5)[10] Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ ($a_0 \neq 0$) be a complex polynomial of degree $n > 1$, and f' its derivative. Let $\alpha_1, \ldots \alpha_n$ be the n roots of f and $\alpha'_1, \ldots, \alpha'_{n-1}$ the $n-1$ roots of the derivative (listing each root as many times as its multiplicity). Show that the *average* of the roots $\alpha_1, \ldots \alpha_n$ of f equals the *average* of the roots $\alpha'_1, \ldots, \alpha'_{n-1}$ of f'. [Hint: Use the relations between the coefficients of a polynomial and the roots of that polynomial.]

(6)[10] Describe (in terms of Jordan form) all 2×2 complex matrices which are similar to their square. [Hint: there are more matrices, Horatio, than are dreamt of in your philosophy!]

(7)[10] (a)[5] Show that the ring of $2n \times 2n$ matrices $M_{2n}(F)$ over a field F for $n \geq 1$ is "algebraically closed" with respect to polynomials of degree 2, in the sense that every polynomial $p(x) = x^2 + \alpha x + \beta \in F[x]$ of degree 2 has a "root" $A \in M_{2n}(F)$ (in the sense that $p(A)$ is the zero matrix). Can you generalize this to polynomials of degree d?

(b)[5] How many real 2×2 matrices $A \in M_2(\mathbb{R})$ are roots of the polynomial $p(x) = x^2 + 1$?

(8)[10] If F is a *finite field* show that every element $\alpha \in F$ is the sum $\alpha = \beta_1^2 + \beta_2^2$ of two squares (for some $\beta_1, \beta_2 \in F$).

(9)[10] If p is a prime number congruent to 1 mod 8, *show* that 2 is a "quadratic residue" mod p, i.e. there is an integer a such that $a^2 \equiv 2$ modulo p. [Hint: show there is an $\varepsilon \in \mathbb{Z}_p$ with $\varepsilon^4 = -1$, and $\alpha^2 = 2$ for $\alpha = \varepsilon + \varepsilon^{-1}$.]

PROOFS

Proof (1): (1) $N_M(P) = M \cap N_G(P)$ (always) $= N_G(P)$ (when $M \supseteq N_G(P)$). (2) Using Sylow on both G and M (noting that P remains a p-Sylow subgroup of M) shows the indexes of the normalizers is congruent to 1, so $[G : N_G(P)] \equiv 1, [M : N_G(P)] = [M : N_M(P)] \equiv 1,\ 1 \equiv [G : N_G(P)] = [G : M][M : N_G(P)] \equiv [G : M]1 = [G : M]$.

Proof (2a): Left-regular representation.

Proof (2b): G_p is in fact the set of all elements of order 1 or p [any element g of order p generates a cyclic subgroup of order p, which by uniqueness must be G_p, therefore $g \in G_p$], hence is invariant under any homomorphism.

Proof (2c): For any $s \in S$ we have $|G| > |S| \geq G \cdot s = [G : Stab(s)]$ (orbit size formula) $= |G|/|Stab(s)|$ so $|Stab(s)| > 1$. Thus $|Stab(s)|$ is a power of p, in particular (by Cauchy) has an element of order p, hence a cyclic subgroup of order p, which by uniqueness must be $G_p : G_p \subseteq Stab(s)$. Thus G_p fixes all points s, thus acts trivially on S.

Proof (3): In $A = \bigoplus Z_{n_i}$, any $x = \sum x_i$ has $x^{n_1} = \sum x_i^{n_1} = 1$ since n_1 is a multiple of n_i, and this is the smallest such power since the generator of Z_{n_1} has order exactly n_1. If m divides n_1 then there exists $Z_m \subseteq Z_{n_1} \subseteq A$. Conversely, if A has an element x of order m then m divides the exponent n_1 (by the above).

Proof (4) The automorphism are precisely all "linear" transformation $\varphi_{a,b}(f(x)) = f(ax+b)$ for invertible a and arbitrary b in R, with inverse $\varphi_{a^{-1},-a^{-1}b}$. Indeed, if $\varphi(x) = f(x), \varphi^{-1}(x) = g(x)$, for f, g of degrees n, m, then $x = \varphi(\varphi^{-1}(x)) = \varphi(g(x)) = g(f(x))$ shows $1 = mn$ (over a domain the degree of the product is $n+m$ and the degree of the composite is nm), so $n = m = 1, f(x) = ax+b, g(x) = cx+d, x = c(ax+b)+d = (ca)x + (cb+d)$ implies $ca = 1$ (so a is invertible with inverse c) and $cb + d = 0$ (so $d = -cb$).

Proof (5): $\frac{1}{n}\sum_{i=1}^{n} \alpha_i = -\frac{1}{n}(\frac{a_{n-1}}{a_n})$, $\frac{1}{n-1}\sum_{i=1}^{n-1} \alpha_i' = -\frac{1}{n-1}(\frac{(n-1)a_{n-1}}{na_n})$.

Proof (6) (1) if the distinct diagonal entries of the Jordan form A are λ, μ then A^2 has diagonal entries λ^2, μ^2 then we either have (1a) $\lambda = \lambda^2, \mu = \mu^2$, so $\lambda, \mu = 0, 1$ and by distinctness $\lambda = 1, \mu = 0$ and we have an idempotent $A \sim \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, or we have (1b) $\lambda = \mu^2, \mu = \lambda^2$, so $\lambda^4 = \lambda \neq 0, 1, \lambda^3 = 1, \lambda = \zeta$ is a primitive cube root of unity and $\mu = \lambda^2 = \lambda^{-1}$, and we have $A \sim \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$. (2) If $A = \lambda I$ then $A^2 = \lambda^2 I$ and we must have $\lambda = \lambda^2$, so again we have idempotents $A = I, 0$. (3) If $A \sim \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ is a 2×2 Jordan block, then $A^2 \sim \begin{pmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda^2 \end{pmatrix}$, so again $\lambda = \lambda^2, \lambda = 1, 0$; but we can't have $\lambda = 0$ (A would be nilpotent of index 2, $A^2 = 0$ nilpotent of index 1, so not similar), hence $A \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $A^2 \sim \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \sim A$.

Proof (7a) Any $p(x)$ has root A consisting of n blocks B_2 strung together down the diagonal (hence the need for even size $2n$), where B_2 is the 2×2 *companion matrix of* $p(x)$, namely $\begin{pmatrix} -\alpha & 1 \\ -\beta & 0 \end{pmatrix}$, and Z_{n-2} the $(n-2) \times (n-2)$ zero matrix. More generally, any polynomial $p(x) = x^d + \alpha_{d-1}x^{d-1} + \ldots + \alpha_1 x + \alpha_0$ has root obtained by duplicating its $d \times d$ companion matrix $n \geq 1$ times to obtain a $dn \times dn$ matrix.

Proof (7b): There are infinitely many distinct conjugates of any solution A, and there is only one Jordan form for a real matrix having minimum polynomial dividing $x^2 + 1$, namely $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ with

rational canonical form $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. [Over the complexes there would be two more conjugacy classes, corresponding to $\pm iI_2$.]

Proof (8): If the characteristic is 2 then the map $\varphi(\alpha) = \alpha^2$ is injective, hence surjective, so every element is a square (and hence trivially $\alpha = \beta^2 = \beta^2 + 0^2$ the sum of two squares). Assume the characteristic is not two, so $\varphi(\alpha) = \varphi(\beta) \Longleftrightarrow (\alpha/\beta)^2 = 1 \Longleftrightarrow \alpha/\beta = \pm 1$ and (except at 0) the map φ is two-to-one; if the size of F is q, then the cardinality of the set $S := \varphi(F)$ of squares is $0 + \frac{1}{2}(q-1) = \frac{q+1}{2}$ (zero together with half of the $q-1$ nonzero values). For any α the sets $\alpha - S$ and S are too big to be disjoint (then F of size q would contain $(\alpha - S) \cup S$ of size $|S| + |S| = q + 1$), so they intersect in some $\alpha - \beta_1^2 = \beta_2^2$.

Proof (9): $\mathbb{Z}_p^\times$ is a cyclic group of order $p-1$ divisible by 8, so it has a unique cyclic subgroup $< \varepsilon >$ of order 8; ε^4 is not 1, yet it is a square root of unity in the field, so it must be -1. The $(\varepsilon + \varepsilon^{-1})^2 = \varepsilon^2 + 2 + \varepsilon^{-2} = 2$ because $\varepsilon^{-2}, \varepsilon^2$ are negatives of each other: both have the same square $(-1)^{-1} = -1$, yet they are not equal (since $\varepsilon^4 \neq 1$), so their quotient squares to 1 but isn't one, and must be the only other square root of unity, namely -1.

Algebra General Exam January 17, 2000

This is exam is worth 100 points. The number of points each part of a problem is worth is indicated in brackets. If you can't prove part of some problem, you can still use the result of that part in proving subsequent parts.

(1)[15] (a)[5] *Define* the trace of an $n \times n$ real matrix, and *show* that the trace of the product XY of two real $n \times n$ matrices is the same as the trace of YX.

(b)[5] *Explain* why the trace of such a matrix is the *sum of all the eigenvalues* (possibly complex, with the appropriate multiplicities) of the matrix.

(c)[5] *Explain* how you would *define* the trace of an abstract *linear operator* on any finite-dimensional real vector space V (i.e., a linear transformation from V to V).

(2)[10] Let K be a field of characteristic zero, $M_n(K)$ the $n \times n$ matrices over K.

(a)[5] *Determine* all linear functionals $f : M_n(K) \longrightarrow K$ which are *symmetric* in the sense that $f(ab) = f(ba)$ for all matrices $a, b \in M_n(K)$.

(a)[5] *Determine* all linear functionals $f : M_n(K) \longrightarrow K$ which are *invariant* in the sense that $f(gag^{-1}) = f(a)$ for all invertible $g \in GL_n(K)$.

(3)[15] (a)[5] Let A be an abelian group, and let f and g be any two endomorphisms of A (group homomorphisms of A into itself). Let $B := \mathrm{Fix}(fg) = \{a \in A \mid f(g(a)) = a\}$, $C := \mathrm{Fix}(gf) = \{a \in A \mid g(f(a)) = a\}$. *Show* that B and C are isomorphic subgroups of A.

(b)[10] *How many* abelian groups (up to isomorphism) are there of order 1000 which have no elements whose orders are larger than 35?

(4)[10] (a)[5] If G is a group containing a cyclic normal subgroup N, *show* that $gn = ng$ for all n in N and all g in the commutator subgroup of G.

(b)[5] Suppose that N_1, N_2, N_3 are three normal subgroups of a group G with the properties that for distinct i, j always $N_i \cap N_j = 1$, $N_i N_j = G$. *Show* that all three subgroups N_i are isomorphic, and that G is abelian. Give an *example* of such an abelian group of order 4.

(5)[10] Let G be a finite group such that every element commutes with its conjugates (for any $g, h \in G$ the elements h and ghg^{-1} commute).

(a)[5] *Show* that any Sylow subgroup of such a G is normal. [Hard!]

(b)[5] *Explain* why the group of quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$ is such a group G.

(6)[10] Given a finite field K, *show* there exists a polynomial $f(x, y) \in K[x, y]$ (in which both variables actually appear) for which the equation $f(x, y) = 0$ has no solutions in $K \times K$.

(7)[15] Suppose that f is an irreducible polynomial of degree n with rational coefficients. Let K be a splitting field for f over the rationals $\mathbb{Q}$, and let $r_1, \ldots, r_n$ be the roots of f in K, with $a = \prod_{i<j}(r_i - r_j)$.

(a)[5] *Show* that the roots of f are distinct.

(b)[5] If the product a is not rational, *show* the Galois group $Gal(K/\mathbb{Q})$ contains an element which yields an odd permutation of the roots.

(c)[5] If the product a is not rational, *show* that K contains at least one quadratic subfield.

(8)[15] Let ζ be primitive 3rd root of unity, $K = \mathbb{Q}$, and $L = K(\sqrt[3]{2})$.

(a)[10] *Show* that L/K is a Galois extension, and *determine* its Galois group $G := Gal(L/K)$.

(b)[5] Considering L as vector space over K, *determine* all K-linear functionals $f : L \to K$ which are G-*invariant* (i.e. $f(\sigma(a)) = f(a)$ for all $\sigma \in G$ and all $a \in L$).

PROOFS

Proof (1):

Proof (2a): Left-regular representation.

Proof (2b):

Proof (2c):

Proof (3):

Proof (4)

Proof (5):

Proof (6)

Proof (7a) Any $p(x)$ has root A consisting of n blocks B_2 strung together down the diagonal (hence the need for even size $2n$), where B_2 is the 2×2 *companion matrix of* $p(x)$, namely $\begin{pmatrix} -\alpha & 1 \\ -\beta & 0 \end{pmatrix}$, and Z_{n-2} the $(n-2) \times (n-2)$ zero matrix. More generally, any polynomial $p(x) = x^d + \alpha_{d-1}x^{d-1} + \ldots + \alpha_1 x + \alpha_0$ has root obtained by duplicating its $d \times d$ companion matrix $n \geq 1$ times to obtain a $dn \times dn$ matrix.

Proof (7b):

Proof (8):

Algebra General Exam

August 18, 2001

(1) If $\phi : G_1 \to G_2$ is a homomorphism of groups, and $N_1 \lhd G_1, N_2 \lhd G_2$ are two normal subgroups, show that the map $\overline{\phi}$ given on cosets by $\overline{\phi}(xN_1) = \phi(x)N_2$ is a well-defined homomorphism $\phi : G_1/N_1 \to G_2/N_2$ of quotient groups *if and only if* the original homomorrphism satisfies $\phi(N_1) \subseteq N_2$.

(2) Show that if p is a prime and H is a subgroup of G, then the number of distinct p-Sylow subgroups of H is less than or equal to the number of distinct p-Sylow subgroups of G.

(3) How many nonisomorphic abelian groups are there of order 325?

(4) If x is an element of a PID R, show that the left R-module R/Rx is irreducible as a *module* if and only if the element x is irreducible as an *element*.

(5) How many non-similar linear transformations T can there be on an 8-dimensional real vector space V having the minimum polynomial $\mu_T(t) = (t-2)(t-3)(t-6)^3$? *List* their Jordan canonical forms.

(6) Consider the transformation T on $\mathbb{R}^3$ which rotates points around the z-axis through a fixed angle θ.

(a) Find the matrix of T with respect to the canonical basis for $\mathbb{R}^3$.

(b) Find the characteristic polynomial of T, and factor it into irreducibles (ignore the cases when θ is an integer multiple of π).

(c) Find the Jordan canonical form for T (you may have to pass to complex matrices).

(7)(a) Show that for any two elements a, b in a cyclic group, at least *one* of the 3 elements a, b, ab is a square (i.e. is of the form x^2 for some element x in the group).

(b) Show that the polynomial $f(x) := (x^2-2)(x^2-3)(x^2-6)$ has no integral roots in $\mathbb{Z}$, but for any prime $p > 0$ it has integral roots modulo p (i.e. the congruence $f(x) \equiv 0 \mod p$ has an integral solution).

(8) Find the Galois group of $f(x) := x^{13} - 1$ over the rationals $\mathbb{Q}$ (i.e. $Gal(K/\mathbb{Q})$ for K the splitting fields of $f(x)$ over $\mathbb{Q}$).

General Exam in Algebra 2002

1. (a) Find all nonconstant polynomials $p(x) \in \mathbb{C}[x]$ satisfying $p(p(p(x))) = p(x)$.
   (b) Find all rational functions $\varphi(x) \in \mathbb{C}(x)$ satisfying $\varphi(2x) = \varphi(x)$.
2. Show that if for a matrix $A \in M_n(K)$ (where K is a field) there exists a nonzero matrix $B \in M_n(K)$ such that $AB = 0$, then there also exists a nonzero matrix $C \in M_n(K)$ such that $CA = 0$ (in other words, in $M_n(K)$ the set of all *left* zero divisors coincides with the set of all *right* zero divisors; notice that $AB = 0$ does **not** always imply $BA = 0$ - find such examples!)
3. Let G be a group. Show that if, for any three elements $x, y, z \in G$, at least two of them commute, then G itself is abelian. (*Hint.* Use centralizers.)
4. Show that a finite group is noncommutative if and only if it has an irreducible complex representation of dimension > 1.
5. Let R be a commutative ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of R. If for all $i \neq j$ we have $\mathfrak{a}_i + \mathfrak{a}_j = R$ then $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$. (*Hint.* Induct, starting from $n = 2$.)
6. Let $R = \mathbb{C}[x, y]/\mathfrak{a}$ where $\mathbb{C}[x, y]$ is the ring of polynomials in variables x and y, and $\mathfrak{a}$ is the principal ideal of $\mathbb{C}[x, y]$ generated by $p(x, y) = y^2 - x^3$. Show that the ideal of R generated by the images of x and y is not principal.
7. Let p be a prime > 2.
   (a) Show that in the symmetric group S_p, any two elements of order p are conjugate.
   (b) Exhibit two nonconjugate elements of order p in the symmetric group S_{p^2}.
   (c) Are there nonconjugate elements of order p in the group $GL_2(\mathbb{C})$? (Recall that $GL_2(K)$, where K is a field, is the group of all nondegenerate 2×2-matrices over K with respect to multiplication.)
   (d) Can you find an element of order p in $GL_2(\mathbb{R})$?
8. Is it true that in the ring R of all continuous functions on $[0, 1]$, any element which is not a zero divisor, is invertible?
9. Construct a Galois extension of $\mathbb{Q}$ of degree 3.

Possible alternative problems

1. Let $p(x) \in \mathbb{R}[x]$ be a polynomial that has only positive values (i.e. $p(\alpha) \geqslant 0$ for any $\alpha \in \mathbb{R}$). Show that $p(x)$ can be written in the form $p(x) = u(x)^2 + v(x)^2$ for some $u(x), v(x) \in \mathbb{R}[x]$ (in other words, $p(x)$ is a sum of two squares in $\mathbb{R}[x]$).
2. Let G be a finite group of order n, and let $r \geqslant 1$ be an integer. Show that the map $\mu_r \colon G \to G$, $\mu_r(x) = x^r$, is surjective (i.e. for every element of G there is an r^{th} root of hat element) if and only if g.c.d$(n, r) = 1$.

3. Let L/K be a field extension in characteristic zero. Suppose there exists an integer $m > 0$ such that $a^m \in K$ for all $a \in L$. Show that $L = K$. (One can give some specific value of m, for example, $m = 3$ or 5.)
4. Let K be a field. A matrix $X \in M_n(K)$ is called *nilpotent* if there exists an integer $m \geqslant 1$ such that $X^m = 0$. Show that if $X \in M_n(K)$ is nilpotent then $X^n = 0$ (where the exponent is the same as the size of X).
5. Find an example of a finite group G such that

   (a) $|\mathrm{Aut}(G)| < |G|$;

   (b) $|\mathrm{Aut}(G)| = |G|$;

   (c) $|\mathrm{Aut}(G)| > |G|$.

   Your work must include a rigorous proof of the fact that the required (in)equality holds.