Department of Mathematics
Algebra Qualifying Exams

(past exams)

ALGEBRA Quals Exam Spring 2013

1. Let G be a finite group with a normal subgroup N such that $C_G(N) \leq N$. Show that

$$|G| \leq |N|!.$$

Also, show that this upper bound is achieved when $|N| = 4$. Identify G in this case.

[Recall that $C_G(N) = \{g \in G : ng = gn \ \forall n \in N\}$.]

2. Let R be a unique factorization domain. Show:

a) For any non-zero $x \in R$, show that there are only finitely many principal ideals containing x.

b) Any ascending chain of principal ideals in R terminates, i.e. if

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq \ldots$$

are ideals in R and each I_k is principal, then there is an integer $n \geq 1$ such that

$$I_n = I_{n+1} = I_{n+2} = \ldots.$$

3. Let V be a finite-dimensional vector space over $\mathbb{Q}$ and let $T : V \to V$ be a linear operator with minimum polynomial $(x^2+1)(x^2-2)$.

Prove:

$$V = U \oplus W$$

where T^2 acts as $-I$ on U and T^2 acts as $2I$ on W.

4. An $n \times n$ matrix U is said to be unipotent if it can be written in the form $I + N$, where I is the identity matrix and N is nilpotent (i.e. $N^k = 0$ for some integer $k \geq 1$). Suppose that U is a unipotent matrix with entries from a field of characteristic p. Show that U has finite order, and that its order is a power of p.

5. Find the splitting field and Galois group of the polynomial

$$x^4 - 2$$

over the field $\mathbb{Q}$.

6. Prove: If F is a field and $GL(n, F)$ is the group of invertible $n \times n$ matrices with entries in F and E is any extension field of F with $[E : F] = n$, then $GL(n, F)$ contains a subgroup isomorphic to $E^\times$, the group of non-zero elements of E under multiplication.

Algebra Quals EXAM Autumn 2012

1. Let G be a finite group and H be a proper subgroup of G. Show

$$\bigcup_{g\in G} g^{-1}Hg \neq G.$$

Hint: This need not be true if G is an infinite group! Try counting and estimating.

2. Let G be a finite group, and P be a Sylow p-subgroup of G. Let H be a subgroup of G containing P: $P \leq H \leq G$. Suppose that P is normal in H and H is normal in G: show P is normal in G.

3. Given: A is a real $n \times n$ matrix such that for any real $n \times n$ matrix B with trace 0 one has $tr(AB) = 0$. Prove that $A = \lambda I$ (for some real scalar λ).

4. Fix a prime p and let $R = R_p$ be the ring

$$\left\{\frac{a}{b} \in \mathbb{Q} \mid gcd(b,p) = 1\right\}.$$

Find all ideals of R and identify those that are prime.

5. Let $R = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$. Let $I = \{a + b\sqrt{-3} \in R \mid a + b \text{ is even}\}$. Show that I is an ideal and determine whether I is a principal ideal.

6. Let $\alpha = \sqrt[5]{2}$ and $\beta = \sqrt{5}$. Let $\gamma = \alpha + \beta$. Show that γ has degree 10 (as an algebraic number over $\mathbb{Q}$).

Algebra Qualifying Exam

Wednesday, March 28, 2012

Jean-François Lafont, Ombudsman

1. Let G be a finite group and H a non-normal subgroup of G of index n. Prove: If $|H|$ is divisible by a prime $p \geq n$, then H is not a simple group.

2. Let A be an abelian subgroup of $GL(n, \mathbb{C})$ of finite exponent m, i.e. $a^m = 1$ for all $a \in A$. Prove: A is a finite group and $|A| \leq m^n$. Also show that this bound is sharp for all m and n.

3. Assume that $A \in M_{n\times n}(\mathbb{C})$ and $rank(A) = 1$. Prove: $det(A + I) = tr(A) + 1$.

4. Let $f(x) \in \mathbb{Q}[x]$ be irreducible of odd degree, and let $F = \mathbb{Q}(\alpha)$, for some root α of $f(x)$. Prove: $F = \mathbb{Q}(\alpha^{2^k})$, for all $k \geq 0$.

5. Given a ring R, let $N(R)$ be the set of nilpotent elements x of R, i.e. those x such that $x^n = 0$ for some $n \in \mathbb{N}$.

   (a) Prove: If R is commutative, then $N(R)$ is an ideal of R.

   (b) Prove or give a counterexample: For any R, $N(R)$ is an ideal of R.

6. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n. Prove: If K is any finite Galois extension of $\mathbb{Q}$, then $f(x)$ factors in $K[x]$ as a product of m irreducible polynomials all of the same degree d (here $md = n$).

Algebra Qualifying Exam

September 21, 2011

Jean-Francois LaFont, Ombudsman

(1) Let $K/\mathbb{Q}$ be a Galois extension whose Galois group is the quaternion group Q_8. Show that K is *not* the splitting field of a quartic polynomial in $\mathbb{Q}[x]$. (**N.B.:** The quaternion group Q_8 is $\{\pm 1, \pm i, \pm j, \pm k\}$, where $i^2 = j^2 = k^2 = ijk = -1$.)

(2) Let $G = \mathrm{SL}(2, F)$, the group of all 2×2 matrices of determinant 1 over a field F. Let G act on the set S of all one dimensional subspaces of F^2 (i.e. S is the set of all lines in F^2 passing through the origin) by $A(< v >) =< v' >$, where $v' = Av$. Prove that G acts doubly transitively on S (i.e., if l, m, l', m' are elements of S with $l \neq m$ and $l' \neq m'$, then there exists $g \in G$ with $g(l) = l'$ and $g(m) = m'$).

(3) Let $a_i \in \mathbb{R}$, $i = 1, 2 \ldots, n$. Let $f(x) = a_1 + a_2 x + \cdots + a_n x^{n-1}$. Prove:

$$\det \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix} = f(\zeta_1) f(\zeta_2) \cdots f(\zeta_n);$$

where $\{\zeta_1, \ldots, \zeta_n\} \subset \mathbb{C}$ are the n-th roots of unity. (**Hint:** Show that $\mathrm{v} := (1, \zeta_i, \zeta_i^2, \ldots)^t$ is an eigenvector for the above matrix for all i.)

(4) We say that a finite group G is supersolvable if G contains a chain of **normal** subgroups:

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G,$$

with $[G_{i+1} : G_i]$ a prime, for all i, $0 \leq i \leq n$. Prove that if G is a finite group of order 2010, then G is supersolvable.

(5) Let $\mathrm{GL}(n, \mathbb{Q})$ be the group of $n \times n$ invertible matrices with rational coefficients. Let G be a finite subgroup of $\mathrm{GL}(n, \mathbb{Q})$ with order divisible by an odd prime p. Prove that $n \geq p - 1$.

(6) Let R be a commutative ring with unit. An element $r \in R$ is nilpotent if and only if $r^n = 0$ for some positive integer n.

(a) Show that the nilpotent elements in R form an ideal (called the "nilradical") which is contained in all prime ideals (in fact, the nilradical *is* the intersection of all prime ideals).

(b) Assume the characterization of the nilradical as the intersection of all prime ideals and let A be an $n \times n$ matrix with coefficients in R. Suppose $A^k = 0$ for some positive integer k. Show that the determinant and trace of A are nilpotent.

Algebra Qualifying Exam

September 21, 2011

Jean-Francois LaFont, Ombudsman

(1) Let $K/\mathbb{Q}$ be a Galois extension whose Galois group is the quaternion group Q_8. Show that K is *not* the splitting field of a quartic polynomial in $\mathbb{Q}[x]$. (**N.B.:** The quaternion group Q_8 is $\{\pm 1, \pm i, \pm j, \pm k\}$, where $i^2 = j^2 = k^2 = ijk = -1$.)

(2) Let $G = \mathrm{SL}(2, F)$, the group of all 2×2 matrices of determinant 1 over a field F. Let G act on the set S of all one dimensional subspaces of F^2 (i.e. S is the set of all lines in F^2 passing through the origin) by $A(< v >) =< v' >$, where $v' = Av$. Prove that G acts doubly transitively on S (i.e., if l, m, l', m' are elements of S with $l \neq m$ and $l' \neq m'$, then there exists $g \in G$ with $g(l) = l'$ and $g(m) = m'$).

(3) Let $a_i \in \mathbb{R}$, $i = 1, 2 \ldots, n$. Let $f(x) = a_1 + a_2 x + \cdots + a_n x^{n-1}$. Prove:

$$\det \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix} = f(\zeta_1) f(\zeta_2) \cdots f(\zeta_n)\,;$$

where $\{\zeta_1, \ldots, \zeta_n\} \subset \mathbb{C}$ are the n-th roots of unity. (**Hint:** Show that $\mathbf{v} := (1, \zeta_i, \zeta_i^2, \ldots)^t$ is an eigenvector for the above matrix for all i.)

(4) We say that a finite group G is supersolvable if G contains a chain of **normal** subgroups:

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G\,,$$

with $[G_{i+1} \colon G_i]$ a prime, for all i, $0 \leq i \leq n$. Prove that if G is a finite group of order 2010, then G is supersolvable.

(5) Let $\mathrm{GL}(n, \mathbb{Q})$ be the group of $n \times n$ invertible matrices with rational coefficients. Let G be a finite subgroup of $\mathrm{GL}(n, \mathbb{Q})$ with order divisible by an odd prime p. Prove that $n \geq p - 1$.

(6) Let R be a commutative ring with unit. An element $r \in R$ is nilpotent if and only if $r^n = 0$ for some positive integer n.

  (a) Show that the nilpotent elements in R form an ideal (called the "nilradical") which is contained in all prime ideals (in fact, the nilradical *is* the intersection of all prime ideals).

  (b) Assume the characterization of the nilradical as the intersection of all prime ideals and let A be an $n \times n$ matrix with coefficients in R. Suppose $A^k = 0$ for some positive integer k. Show that the determinant and trace of A are nilpotent.

Algebra Qualifying Exam

Wednesday, March 30, 2011

Jean-François Lafont, Ombudsman

1. Let G be a finite group with $|G| = p^2q$, where p and q are primes and $p < q$. Prove: Either G has a normal Sylow q-subgroup or $G \cong A_4$, the alternating group of degree 4.

2. Let p be a prime and R a ring with identity $1 \neq 0$. Prove: If $|R| = p^2$, then R is a commutative ring.

3. Let R be a principal ideal domain and let $I, J \leq R$ be nonzero ideals of R. Prove: $IJ = I \cap J$ if and only if $I + J = R$.

4. Let $a, b \in \mathbf{C}$ and let $A : \mathbf{C} \to \mathbf{C}$ be defined by $A(z) = az + b\overline{z}$, for $z \in \mathbf{C}$. Prove that A is invertible if and only if $|a| \neq |b|$.

5. Let A be an $n \times n$ matrix over $\mathbf{C}$. Prove that A and A^t are conjugate. [Note: A^t denotes the transpose of the matrix A.]

6. Let $K/\mathbf{Q}$ be the splitting field for the polynomial $f(x) = x^4 - 3x^2 + 4$. Find the Galois group of $K/\mathbf{Q}$, as well as all of its subgroups and the corresponding field extensions. [Hint: Note that $(\frac{1+\sqrt{-7}}{2})^2 = \frac{-3+\sqrt{-7}}{2}$.]

Algebra Qualifying Exam

Monday, September 20, 2010

Ron Solomon, Ombudsman

1. Suppose that G is a group, and H is a nontrivial subgroup such that $H \leq J$ for *every* nontrivial subgroup J of G. Show that H is contained in the center of G.

2. Let G be a transitive subgroup of $Sym(X)$, the symmetric group on the set X. Let N be a normal subgroup of G, $N \neq 1$. Show that N has no fixed points in X, i.e. there is no $x \in X$ such that $hx = x$ for all $h \in N$.

3. Let A, B be two $n \times n$ complex matrices, and assume $AB = BA$. Prove that A, B have a common eigenvector.

4. Let $F \subseteq K \subseteq L$ be a tower of fields, and suppose that K/F and L/K are algebraic (but not necessarily finite) extensions. Does L/F have to be algebraic? Give a proof or counterexample.

5. Let $\mathbb{Z}[i]$ be the ring of Gaussian integers.

   (a) Show that 3 is prime in $\mathbb{Z}[i]$ but 5 is not.

   (b) Show that, if a prime p in $\mathbb{Z}$ is not prime in $\mathbb{Z}[i]$, then either $p = 2$ or $p \equiv 1 \pmod 4$.

6. Let $n, m \geq 1$ be positive integers with greatest common divisor d. Show that the ideal of $\mathbb{Q}[x]$ generated by $x^n - 1$ and $x^m - 1$ is principal and generated by $x^d - 1$.

Algebra Qualifying Exam

Wednesday, March 31, 2010

Warren Sinnott, Ombudsman

1. Let p be a prime, and let P be a finite p-group. Suppose that $Q \leq P$ is a proper subgroup. Show that $N(Q) \neq Q$.

2. Let G be a finite group with commutator subgroup G'. Let N be the subgroup of G generated by the set $\{x^2 \mid x \in G\}$. Prove that N is a normal subgroup of G and N contains G'.

3. Let A be an $m \times n$ real-valued matrix and let A^T denote its transpose. Prove that $\operatorname{rank}(A^TA) = \operatorname{rank}(A)$. (*Hint.* Prove that A^TA and A have the same nullspace.)

4. Suppose that I is an ideal in $\mathbf{Z}[x]$ generated by a prime number p and a polynomial $f(x)$. Prove that I is maximal if and only if $f(x)$ is irreducible mod p.

5. Construct two Galois extensions of degree four of the field of rational numbers $\mathbf{Q}$, one with Galois group $Z_2 \times Z_2$ and one with Galois group Z_4. Prove that your constructions possess the required properties.

6. (a) Let $F = \{a + b\sqrt{-7} : a, b \in \mathbf{Q}\}$: show that F is a field.

   (b) Show that $F \simeq \mathbf{Q}[x]/(x^2 + 7)$.

Algebra Qualifying Exam

Monday, September 21, 2009

Paul Ponomarev, Ombudsman

1. Let G be a finite group of order pq^2, where $p \neq q$ are primes and p doesn't divide $\#Aut(G)$, the order of the automorphism group of G. Prove that G is abelian.

2. Let G be an abelian subgroup of the symmetric group $Sym(X)$ on a set X. Suppose that G acts transitively on X. Show that the stabilizer G_x is trivial for every $x \in X$.

3. Let V be a finite-dimensional vector space over $\mathbb{Q}$ and
$$T : V \to V$$
a linear transformation satisfying
$$T^2 = -I$$
where I is the identity transformation of V. Suppose one knows that V has a non-trivial proper subspace W that is invariant under T. (Here "non-trivial proper" means that $W \neq \{0\}$ and $W \neq V$.) What is the smallest that $\dim_{\mathbb{Q}} V$ could be? Justify your answer.

4. Let $R = \mathbb{Z}[\sqrt{-m}] = \{a + b\sqrt{-m} : a, b \in \mathbb{Z}\}$ where m is a square-free odd integer with $m \geq 3$.
   (a) Find all units of R.
   (b) Show that 2 and $1 + \sqrt{-m}$ are irreducible in R.
   (c) Show that R is not a unique factorization domain.
   (*Hint:* The function $\mathbf{N} : R \to \mathbb{Z}$ defined by $\mathbf{N}(a + b\sqrt{-m}) = a^2 + b^2 m$ is useful.)

5. Let $K = \mathbb{Q}(\zeta_8)$ with $\zeta_8 = e^{2\pi i/8}$. Determine $G = Gal(K/\mathbb{Q})$. For each proper subgroup H of G find the fixed field K^H and find an element $\alpha \in K$ such that $K^H = \mathbb{Q}(\alpha)$.

6. Show that every algebraically closed field must be infinite.

Algebra Qualifying Exam, Spring 2009

1. Show that any group of order $2^2 \cdot 3^m$ is solvable.

2. Suppose finite group G has normal subgroups $A, B \leq G$ such that $A \cap B = \{e\}$, where e is the identity element.
Assume the truth of the following statements:

(i) AB is a subgroup.

(ii) $ab = ba$ whenever $a \in A$ and $b \in B$.

(iii) Every $g \in AB$ can be expressed *uniquely* as a product $g = ab$ for some $a \in A$ and $b \in B$.

(iv) The four subgroups $\{e\}$, A, B, and AB are normal in AB.

Suppose A and B are simple groups, and there exists a normal subgroup $N \trianglelefteq AB$ that is *not* equal to one of the four subgroups listed in (iv) above.
Prove: The groups A and B must be isomorphic.

3. Suppose I is an ideal of $R = \mathbb{Z}[x]$ and $p \in I$ for some prime number p. Show that I can be generated by 2 elements.

4. Suppose $f(x) \in K[x]$ is an irreducible polynomial of degree n over the field K. Suppose L/K is a field extension with finite degree $[L : K] = m$. If m, n are relatively prime, prove: $f(x)$ is irreducible in $L[x]$.

5. Let $K \subseteq \mathbb{C}$ be the splitting field of $X^p - 2$ over $\mathbb{Q}$, where p is a prime. Let $\alpha \in \mathbb{C}$ be a root of $X^p - 2$ and let ζ be a primitive p-th root of unity.

(a) If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, show that

$$\sigma(\alpha) = \zeta^{c(\sigma)}\alpha \quad \text{and} \quad \sigma(\zeta) = \zeta^{d(\sigma)}$$

for some $c(\sigma) \in \mathbb{Z}/(p)$, $d(\sigma) \in (\mathbb{Z}/(p))^*$.

(b) Define $\varphi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/(p))$ by: $\varphi(\sigma) = \begin{bmatrix} 1 & 0 \\ c(\sigma) & d(\sigma) \end{bmatrix}$.

Prove: φ is a group homomorphism, and its image is the set of all matrices in $\mathrm{GL}_2(\mathbb{Z}/(p))$ having the form $\begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix}$.

6. Suppose $T : \mathbb{R}^4 \to \mathbb{R}^4$ is a linear transformation whose fourth power is minus the identity map.

(a) What are possible eigenvalues of T (in the field $\mathbb{C}$ of complex numbers)? What are its possible Jordan canonical forms over $\mathbb{C}$?

(b) A subspace $V \subseteq \mathbb{R}^4$ is T-invariant if $T(V) = V$.
Must there exist T-invariant subspaces of $\mathbb{R}^4$, other than $\{0\}$ and $\mathbb{R}^4$?
If not, say why not. If so, identify the invariant subspaces.

Algebra Qualifying Exam

Monday, September 22, 2008

Dan Shapiro, Ombudsman

1. Show that any finite group G of order 224 has a subgroup of order 28.

2. For each pair of groups from the following list, decide whether they are isomorphic or not:

(a). the multiplicative group of the integers mod 13

(b). the multiplicative group of the integers mod 28

(c). the alternating group on 4 letters

(d). the group of symmetries of the regular hexagon

Justify your answers.

3. Let A be an $n \times n$ complex matrix. Prove that $A^m = 0$ for some positive integer m if and only if all eigenvalues of A are 0.

4. Let R be a commutative ring with identity, and let A and B be ideals of R. Suppose that I is an ideal of R contained in $A \cup B$. Show that $I \subseteq A$ or $I \subseteq B$.

5. Let $\alpha = 2\cos\left(\frac{2\pi}{7}\right)$. Find the minimal polynomial of α over $\mathbb{Q}$, the splitting field F of this polynomial over $\mathbb{Q}$, and determine the Galois group of F over $\mathbb{Q}$.

6. For a prime p, let F_p denote the field with p elements. Let $q = p^n$ for some integer $n \geq 1$.

(a) Show that up to isomorphism there exists a unique field F_q containing q elements.

(b) Compute the Galois group $Gal(F_q/F_p)$. Justify your answer.

Algebra Qualifying Exam
March 26th, 2008
Paul Ponomarev, Ombudsman

1. Show that the symmetric group S_5 has six Sylow 5-subgroups. Deduce that S_6 contains two subgroups that are isomorphic to S_5 but that are not conjugate to each other. You may assume that the only normal subgroups of S_5 are 1, A_5 and S_5. (Hint: the action of S_5 on its Sylow 5-subgroups gives a homomorphism $\phi : S_5 \to S_6$.)

2. Show that for $n \geq 3$, the center of the symmetric group S_n is trivial.

3. Let $\lambda = (3+\sqrt{5})/2$. Find the Jordan normal form for the following matrix.

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

4. Let K be an extension of $\mathbb{Q}$ contained in $\mathbb{C}$ such that $K/\mathbb{Q}$ is Galois and $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order 4. Show that $i \notin K$. (Hint: complex conjugation defines an automorphism of K.)

5. Recall that a nilpotent element of a ring R is a nonzero element a such that $a^n = 0$ for some $n > 0$, and that an idempotent element is a nonzero element e such that $e^2 = e$. Let k be a field and let I be a nonzero ideal in $k[x]$, the ring of polynomials over k. Suppose that the quotient ring $R = k[x]/I$ contains no nilpotent elements and contains no idempotents except 1. Show that R is a field. (Hint: Use the Chinese remainder theorem.)

6. Let $R = \mathbb{Z}[\sqrt{-3}]$ and let $S = \mathbb{Z}[i]$. Show that there is no unital ring homomorphism $\phi : R \to S$. (Recall that 'ϕ is unital' means that ϕ satisfies $\phi(1_R) = 1_S$.)

Algebra Qualifying Exam

Monday, September 17, 2007

1. Let G be a group, and suppose that G has a normal subgroup N of order p (where p is a prime). Let g be an element of G: show that N is contained in the centralizer of g^{p-1}.

2. Let K be a subfield of the complex numbers $\mathbb{C}$, and let p be a prime. Suppose that *every* proper finite extension of K in $\mathbb{C}$ has degree divisible by p. Show that every finite extension of K in $\mathbb{C}$ has degree a power of p. (Hint: this problem uses the Sylow Theorems in addition to Galois Theory.)

3. (a) Is $(5, x^2 + 1)$ a prime ideal in $\mathbb{Z}[x]$?

   (b) Is $(5, x^3 + x + 1)$ a prime ideal in $\mathbb{Z}[x]$?

   Justify your answers.

4. Suppose that $f(x, y) \in K[x, y]$ is a polynomial in two variables with coefficients in an infinite field K. Suppose that $f(c, c) = 0$ for every $c \in K$.

   Prove: $x - y$ is a factor of $f(x, y)$, i.e. $f(x, y) = (x - y)q(x, y)$ for some $q(x, y) \in K[x, y]$.

5. Let A be an $n \times n$ matrix, with all diagonal entries equal to c and all off-diagonal entries equal to 1. Compute $det(A)$.

6. Suppose A is an $n \times n$ matrix over a field K with minimal polynomial $m_A(x)$. Let $f(x) \in K[x]$ be a polynomial. Prove: $f(A)$ is nonsingular $\iff$ $f(x)$ and $m_A(x)$ are relatively prime in $K[x]$.

Algebra Qualifying Exam
March 26, 2007
Vitaly Bergelson, Ombudsman

1. Let G be a nonabelian finite group and let $n > 1$. Prove: If every maximal proper subgroup of G has index n in G, then $n = p$ is a prime and G is a p-group. (Hint: Think Sylow.)

2. Let G be a group with commutator subgroup $[G, G]$. Let N be the subgroup of G generated by $\{x^2 : x \in G\}$. Prove: N is a normal subgroup of G containing $[G, G]$.

3. Determine the rational canonical form and a Jordan canonical form for the matrix
$$\begin{pmatrix} 6 & -8 & 0 & 3 \\ 5 & -7 & 0 & 3 \\ 2 & -3 & 1 & 1 \\ 5 & -8 & 0 & 4 \end{pmatrix}.$$

4. Let k be a field, $M = M(n, k)$ the ring of $n \times n$ matrices over k, and $G = GL(n, k)$ the group of invertible elements of M. For X a subset of M, let
$$C_M(X) = \{T \in M : ST = TS \text{ for all } S \in X\}.$$
Let $C_G(X)$ be defined analogously.
   (a) Prove: $C_M(X)$ is a k-vector subspace of M for all subsets X of M.
   (b) Suppose $X_r \subseteq \cdots \subseteq X_2 \subseteq X_1$ is a chain of subsets of G such that
$$C_1 \subsetneq C_2 \subsetneq \cdots \subsetneq C_r \text{ (proper containments)}$$
where $C_i = C_G(X_i), 1 \leq i \leq r$. Prove: $r \leq n^2$.

5. Let R be an integral domain with quotient field F. Let $p(x) \in R[x]$ be a monic polynomial. Suppose that $p(x) = a(x)b(x)$ with $a(x), b(x)$ monic polynomials in $F[x]$.
   (a) Prove: If $a(x)$ is not in $R[x]$, then R is not a UFD.
   (b) Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

6. Prove: Let $f(x) \in \mathbb{Q}[x]$ be irreducible with splitting field K over $\mathbb{Q}$. Suppose that the Galois group of $K/\mathbb{Q}$ is abelian. Then $K = \mathbb{Q}(\alpha)$ for any root α of $f(x)$ in K.

Algebra Qualifying Exam
Sept. 20, 2006

1. (a) Prove: let G be a group having a subgroup H of index m. Then G has a normal subgroup N whose index $[G : N]$ is a *multiple* of m and a *divisor* of $m!$.

   (b) Let $f(x) \in \mathbb{Q}[x]$ be irreducible of degree n, and suppose that the Galois group of f is A_n (the alternating group on n letters). Let α be a root of $f(x)$ in $\mathbb{C}$. Prove: there is no field F strictly between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$. (Use (a)).

2. Let p and q be primes with $p < q$. Prove: If G is a group with $|G| = p^2q$, then either G has a normal subgroup of order q or $G \simeq A_4$ (the alternating group on 4 letters).

3. Let R be a commutative ring with 1.

   (a) Show that every maximal ideal of R is prime.

   (b) If R is a PID, show that every prime ideal is maximal.

   (c) Give an example of a commutative ring R with 1 and an ideal $I \subseteq R$ such that I is prime but not maximal.

4. Let F be a field of characteristic 0 containing the n-th roots of unity, and let b be an element of F. Let K be an extension of F generated by an n-th root β of b: $\beta^n = b$ and $K = F(\beta)$.

   (a) Show that K is the splitting field over F of the polynomial $x^n - b$.

   (b) Show that $G = Gal(K/F)$ is cyclic of order dividing n.

5. Let V be a finite-dimensional vector space over a field F. Suppose $T : V \to V$ is a cyclic linear transformation, i.e., there exists $v \in V$ such that $\{v, T(v), \ldots, T^{n-1}(v)\}$ is a basis for V over F (here n is the dimension of V). Let $S : V \to V$ be a linear transformation that commutes with T. Prove that S is a polynomial in T: $S = p(T)$ for some polynomial $p(x)$ in $F[x]$.

6. Let R be the ring of $n \times n$ matrices over a field F. Show that every nonzero element of R is either a unit or a zero-divisor.

Algebra Qualifying Exam
March 29, 2006

1. Let F be a field and let $p(x)$ be a non-constant, not necessarily irreducible polynomial with coefficients in F. Show that there exists an extension field E/F where $p(x)$ has a root.

2. Let V be a non-trivial vector space, let $T\colon V \longrightarrow V$ be a linear transformation, and suppose that there are no T-stable subspaces of V other than 0 and V itself. Show that the ring of all linear endomorphisms of V which commute with T forms a division ring (skew field); i.e., a not necessarily commutative field.

3. In the ring $\mathbb{Q}[X,Y]$ find a finite set of generators for the ideal $I := \{f(X,Y) \in \mathbb{Q}[X,Y] \mid f(i,i) = 0\}$ (where $i^2 = -1$ as usual). (**Hint:** What are some obvious polynomials in $\mathbb{Q}[X,Y]$ which vanish at the point (i,i)? Try to show that these polynomials generate I.)

4. Let K/k be a finite Galois extension of fields. The *norm map* from K^* to k^* is defined by $\mathrm{N}_{K/k}(\alpha) := \prod_\sigma \sigma(\alpha)$ where σ runs over the elements of the Galois group.

   (a) Show that the norm is a homomorphism of groups.

   (b) Now let K/k be an extension of degree n of finite fields. Let q be the cardinality of k. Show that
   $$\mathrm{N}_{K/k}(\alpha) = \alpha^{(q^n-1)/(q-1)}$$
   for $\alpha \in K^*$.

   (c) Let K/k be as in part (b). Show that $\mathrm{N}_{K/k}\colon K^* \to k^*$ is surjective.

5. (a) List all abelian groups of order 28 up to isomorphism.

   (b) Can a group of order 28 be simple? Prove your answer.

   (c) Construct two non-isomorphic non-abelian groups of order 28.

6. Let $\mathbb{C}$ be the complex numbers and set $V := \mathbb{C}^4$. Let S and T be two endomorphisms of V whose matrices with respect to the canonical basis $B := \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$ are
$$[T]_B = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$
and
$$[S]_B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$
Find a basis B' of V which simultaneously diagonalizes T and S. Justify your answer.

Algebra Qualifying Exam
Wednesday, September 21, 2005
Dan Shapiro, Ombudsman

1. Let V be a vector space over a field F. Let $P : V \to V$ be a *projection*, that is, a linear transformation such that $P^2 = P$.

   (a) Show that $V = \mathrm{im}P \oplus \ker P$. ($\mathrm{im}P$ is the image of P, also called the range; $\ker P$ is the kernel of P, also called the nullspace.)

   (b) If V is finite dimensional and P and Q are two commuting projections, so $PQ = QP$, show that V has a basis with respect to which both P and Q are represented by diagonal matrices.

2. Let V be a finite dimensional vector space over a field F, $T : V \to V$ a linear transformation. Show that V can be written as a direct sum $V = U \oplus W$, where U, W are subspaces, stable under T, such that $T|_U$ is invertible and $T|_W$ is nilpotent (this means that $(T|_W)^k$ is 0 for some integer $k > 0$).

3. Suppose that G is a finite group and N is a normal subgroup of order p, where p is the smallest prime dividing the order of G. Show that N is contained in the center of G.

4. (a) Show that S_5 is generated by (12) and (12345).

   (b) Let $f(x)$ be an irreducible quintic in $\mathbb{Q}[x]$ with exactly two non-real roots. Show that the Galois group of f is S_5.

5. Let I be the ideal generated by 3 and $x^3 + x^2 + 1$ in $\mathbb{Z}[x]$.

   (a) Prove or disprove: I is a principal ideal.

   (b) Prove or disprove: I is a prime ideal.

6. Let R be a commutative ring with identity, and let J be the intersection of all maximal ideals of R: show that $1 + J = \{1 + x : x \in J\}$ is a subgroup of the group of units of R. (Hint: you may assume the result that every ideal $I \neq R$ is contained in a maximal ideal of R.)

Algebra Qualifying Exam
Spring 2005

1. Prove: Let G be a finite simple group having a subgroup H of prime index p (i.e., $(G : H) = p$). Then p is the largest prime divisor of $|G|$.

2. Let $\mathbf{C}$ denote the complex numbers and let $G = GL(2, \mathbf{C})$ be the group of all invertible 2×2 matrices with complex entries. We call a subgroup H of G diagonalizable if there exists a matrix $t \in G$ such that tht^{-1} is a diagonal matrix for all $h \in H$, i.e., tHt^{-1} is a subgroup of the group of diagonal matrices in G.

(a) Prove: Any finite abelian subgroup A of $GL(2, \mathbf{C})$ is diagonalizable. (Hint: First prove that elements of finite order in G are diagonalizable.)

(b) Give an example of an infinite abelian subgroup of $GL(2, \mathbf{C})$ which is not diagonalizable. Justify your claim briefly.

(c) Give an example of a finite subgroup H of $GL(2, \mathbf{C})$ which is not diagonalizable. Justify your claim briefly.

3. Let p be a prime number and let n be a natural number. Let $\mathbf{Q}$ denote the field of rational numbers and let $V = \mathbf{Q}^n$ denote the n-dimensional vector space of column vectors with entries from $\mathbf{Q}$. Let

$$A = \begin{pmatrix} 0 & . & . & . & p \\ 1 & 0 & . & . & 0 \\ 0 & 1 & . & . & 0 \\ . & . & . & . & . \\ 0 & . & . & 1 & 0 \end{pmatrix}$$

be an $n \times n$-matrix, and let $T : V \to V$ be the linear transformation $T(v) = Av$ for all $v \in V$.

(a) Find the minimum polynomial of T, and justify your claim briefly.

(b) Prove: V has no proper, non-trivial T-invariant subspaces.

4. (a) Let R be a PID and let P be a non-0 prime ideal of R. Prove: R/P is a field.

(b) Give an example of a UFD S and a non-0 prime ideal Q of S such that S/Q is not a field.

5. Let R be a commutative ring with identity. For an ideal I of R, define

$$V_I = \{P | P \text{ is a prime ideal of } R \text{ and } I \subseteq P\}.$$

Let I and J be ideals of R. Let IJ denote the ideal of R generated by $\{ab | a \in I; b \in J\}$.

a) Prove : $V_I \cap V_J = V_{I+J}$.

b) Prove: $V_I \cup V_J = V_{IJ} = V_{I \cap J}$. (Hint: Show $V_I \cup V_J \subseteq V_{I \cap J} \subseteq V_{IJ} \subseteq V_I \cup V_J$.)

6. Let p be a prime and let $F = \mathbf{F}_p$ be the finite field of cardinality p. Let $a \in F$ with $a \neq 0$. Let E be the splitting field of $g(x) = x^p - x + a$ over F.

a) Find all of the roots of $g(x)$ in E. (Hint: Consider the difference $\alpha - \beta$ of any two roots of $g(x)$.)

b) Prove: $g(x)$ is irreducible over F.

c) Find all of the automorphisms of the field E, and identify the automorphism group of E.

Algebra Qualifying Exam
Autumn 2004

1. Let $\alpha = \sqrt{5+\sqrt{5}}$ and let $K = \mathbb{Q}(\alpha)$.
   (a) Find the minimal polynomial $m(x)$ of α over $\mathbb{Q}$, and show that K is the splitting field of $m(x)$.
   (b) Show that there is an automorphism $\sigma \in Gal(K/\mathbb{Q})$ such that $\sigma(\alpha) = \alpha'$, where $\alpha' = \sqrt{5-\sqrt{5}}$. Show $\sigma(\sqrt{5}) = -\sqrt{5}$ and that $\sigma^2(\alpha) = -\alpha$.
   (c) Show that $Gal(K/\mathbb{Q})$ is cyclic.

2. Let A be an $n \times n$ matrix with complex entries and let $\lambda_1, \ldots, \lambda_n$ be its eigenvalues, counted with multiplicity. Let $p(x)$ be any polynomial in $\mathbb{C}[x]$.
   (a) Show that the determinant of $p(A)$ is $\prod_{k=1}^{n} p(\lambda_k)$.
   (b) Show that the trace of $p(A)$ is $\sum_{k=1}^{n} p(\lambda_k)$.

   Hint: Show first that we can assume that A is in Jordan Canonical Form.

3. Let F be a field and let f, g be distinct irreducible polynomials of $F[x]$.
   (a) Describe the ideals of the ring $F[x]/(f^2 g)$.
   (b) Show that there does not exist a surjective ring homomorphism from $F[x]/(f^3)$ to $F[x]/(f^2 g)$

4. Let G be a finite group and let p be the smallest prime divisor of the group order $|G|$. Show that every subgroup H of index p in G is normal in G.

5. Let G be a group such that G/Z is cyclic. Show that G is abelian. (Here Z is the center of G.)

6. Suppose that $\{E_1, E_2, \cdots, E_t\}$ is a set of non-zero 4×4 matrices with complex entries satisfying: $E_i^2 = E_i$ and $E_i E_j = E_j E_i = 0$ for all i, j, $1 \leq i, j \leq t$, $i \neq j$.

   Prove : $t \leq 4$. (Hint: Show that commuting diagonalizable matrices can be simultaneously diagonalized.)

Algebra Qualifying Exam
Spring 2004

1. Let G be a finite group with $|G| = p^a n$, where p is a prime and a and n are natural numbers with $p < n < 2p$.

   (a) Prove: If $a > 1$, then G has a normal p-subgroup P with $|P| > 1$. (Hint: Consider the permutation action of G on the left cosets of a suitable subgroup of G.)

   (b) Give an example of a group G with $|G| = pn$ with $p < n < 2p$ such that G does not have a normal Sylow p-subgroup.

2. (a) Let A and B be two commuting $n \times n$ real matrices with $A^2 = B^2 = I$, where I is the identity $n \times n$ matrix. Prove that A and B are simultaneously diagonalizable, i.e., that there is an invertible $n \times n$ real matrix P such that both PAP^{-1} and PBP^{-1} are diagonal matrices.

   (b) Prove: If H is a Klein 4-subgroup of $GL(2, \mathbb{R})$ (i.e. H is a non-cyclic subgroup with $|H| = 4$), then H is conjugate to a unique diagonal subgroup of $GL(2, \mathbb{R})$. (Hint: Use (a).)

   (c) Prove: $GL(2, \mathbb{R})$ contains no subgroup isomorphic to A_4, the alternating group on $\{1, 2, 3, 4\}$. (Hint: Use (b). What is the center of A_4?)

3. Let V be a finite-dimensional vector space over $\mathbb{F}_2$, the field of two elements. Let $T : V \to V$ be a non-singular linear transformation such that $T^5 = I$ but $T \neq I$.

   (a) Show that the minimum polynomial of T has degree either 4 or 5.

   (b) What is the smallest possible dimension of V for which there are two non-similar non-identity linear transformations $T : V \to V$ and $S : V \to V$ with $T^5 = I = S^5$? Explain.

4. Let c be a complex number and let R be the ring of all complex numbers which can be written as a polynomial in c with rational coefficients. Prove that c is algebraic if and only if R is a field.

5. Let p be a prime number and let R be the set of all rational numbers with denominator prime to p. R is a subring of $\mathbb{Q}$.

   (a) What are the units of R?

   (b) Show that R is a principal ideal domain.

   (c) Show that R has a unique maximal ideal M, find a generator for M, and identify R/M.

6. Let F be the splitting field of $x^4 + 1$ over $\mathbb{Q}$.

   (a) Find the Galois group of F over $\mathbb{Q}$.

   (b) Find all the quadratic subfields of F.

Algebra Qualifying Exam
Autumn 2003

1. There are five nonisomorphic groups of order 12 (you may take this as given). List them all, and show that the groups you list are mutually nonisomorphic.

2. Let G be a finite group, let x, y be distinct elements of G of order 2, and let $H = < x, y >$.

   (a) Show that H is a dihedral group.

   (b) Suppose x and y are not conjugate in G. Show that the order of H is divisible 4 and the center of H is nontrivial.

   Note: A dihedral group D_{2n} of order $2n$ is defined as follows.

   $$D_{2n} = < a, b | a^2 = b^n = 1, aba = b^{-1} > .$$

3. Suppose that P is a prime ideal of a commutative ring R (with identity)and let I and J be ideals of R. Let IJ be the ideal of R generated by all products ij where $i \in I, j \in J$.

   (a) Suppose that $IJ \subseteq P$: show that either $I \subseteq P$ or $J \subseteq P$.

   (b) Suppose that $I \cap J \subseteq P$: show that either $I \subseteq P$ or $J \subseteq P$. (Use (a)).

4. (a) Show that every integral domain which is also a finite set is actually a field.

   (b) Use part (a) to show that every non-trivial prime ideal of $\mathbb{F}_p[x]$ is actually maximal. (Here $\mathbb{F}_p$ is the finite field with p elements.)

5. (a) Let $L \subseteq \mathbb{C}$ be a finite Galois extension of $\mathbb{Q}$ with Galois group G. Suppose that G has odd order. Show that $L \subset \mathbb{R}$.

   (b) Is the converse true? I.e. if $L \subseteq \mathbb{R}$ is a finite Galois extension of $\mathbb{Q}$ with Galois group G, must the order of G be odd?

   (c) Give an explicit example of an extension $L \subseteq \mathbb{C}$ of degree 3 which is *not* contained in $\mathbb{R}$.

6. Let A, B be complex $n \times n$ matrices such that $AB = BA$.

   (a) Suppose that $v \in \mathbb{C}^n$ is an eigenvector of A with eigenvalue λ: show that Bv is either 0 or an eigenvector of A with eigenvalue λ.

   (b) Suppose that A has n distinct eigenvalues. Show that B is diagonalizable.

Algebra Qualifying Exam, Spring 2003

1. Let p be a prime dividing the order of a finite group G. Show that G contains an element of order p without using Sylow's theorem. (Suggestion: Use the class equation and an inductive argument.)

2. Let G be a group. For $a, b \in G$ put $a^b = b^{-1}ab$, $[a,b] = a^{-1}b^{-1}ab$.

   (i) Show that $[a, bc] = [a,c][a,b]^c$ for $a, b, c \in G$.

   (ii) Suppose that $G = AB$, where A, B are subgroups of G. Let $[A, B]$ denote the subgroup of G generated by all $[a,b]$, where $a \in A$, $b \in B$. Show that $[A, B]$ is a normal subgroup of G.

   (iii) Suppose, in addition, that A and B are abelian. Show that $G/[A,B]$ is abelian and $[G,G] = [A,B]$.

3. Let $R = k[X,Y]$, where X, Y are independent indeterminates over the field k. Let $p = p(X)$ be an irreducible polynomial in $k[X]$. Put $F = k[X]/(p)$.

   (i) Show that pR is a prime ideal of R but not a maximal ideal of R.

   (ii) Determine all the maximal ideals of $F[Y]$.

   (iii) Determine all the maximal ideals of R containing pR.

4. Classify, up to similarity by real matrices, all 7×7 real matrices having characteristic polynomial $X^3(X^2+1)^2$.

5. Let K be a splitting field of $X^3 - 3$ over $\mathbb{Q}$.

   (i) Determine the Galois group of K over $\mathbb{Q}$.

   (ii) Give an example of a subfield E of $\mathbb{C}$ such that $[E(\sqrt[3]{3}) : E] = 2$.

6. Find an element $\alpha \in \mathbb{C}$ such that:

   (i) $\mathbb{Q}(\alpha)$ is a normal extension of degree 4 over $\mathbb{Q}$ whose Galois group over $\mathbb{Q}$ is cyclic.

   (ii) $\mathbb{Q}(\alpha)$ is a normal extension of degree 5 over $\mathbb{Q}$.

Qualifying Exam
Algebra
Aut 2002

9/23/02

CODE NAME :

[1]. Let G be a group defined by

$$G = \langle a, b | a^4 = b^3 = 1, ba = ab^{-1} \rangle.$$

(i). Find the order $|G|$ of G.
(ii). For each divisor d of $|G|$, find the number of elements of order d in G.

CODE NAME :

[2]. Let a, b be 5-cycles defined by

$$a = (12345), b = (13524).$$

(i). Show that the centralizer of a in S_5 is the cyclic group generated by a.
(ii). Show that a and b are not conjugate in A_5.

CODE NAME :

[3]. Let

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

(a). Find the characteristic polynomial and the minimal polynomial of A.
(b). Find all eigenvalues for A.
(c). For each eigenvalue λ, find a basis for the corresponding eigenspace.
(d). Is A diagonalizable ? Justify.

CODE NAME :

[4]. For each pair of rings from the list below, decide which are isomorphic. Give a brief justification for your answer. In this problem $M_k(R)$ is the ring of $k \times k$ matrices over the ring R, and $\mathbb{Z}_n$ is the ring of integers mod n.
(a). $M_2(F)$, where F is the field with 4 elements.
(b). $M_2(\mathbb{Z}_4)$.
(c). $\mathbb{Z}_{16} \oplus \mathbb{Z}_{16}$.
(d). $\mathbb{Z}_4 \oplus \mathbb{Z}_{64}$.

CODE NAME :

[5]. Let K be the splitting field of $X^4 - 3$ over $\mathbb{Q}$.
(a). Determine the Galois group of $K/\mathbb{Q}$.
(b). Determine all the quadratic subfields of K over $\mathbb{Q}$ and their corresponding subgroups under the Galois correspondence.
(c). Find all subfields F of K such that $[F : \mathbb{Q}] = 4$ and F is Galois over $\mathbb{Q}$.

CODE NAME :

[6]. Let F be a finite field with q elements and $a \in F^{\times}$. Assume that $q \equiv 1 \pmod 3$. Show that $X^3 - a$ is irreducible over F if and only if $a^{\frac{q-1}{3}} \neq 1$.

Spring 2002 Algebra Qualifier

1. (a) Show that the alternating group A_4 of degree 4 has order 12.
   (b) Show that A_4 does not contain a subgroup of order 6.

2. Let $K = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/7}$. The minimal polynomial of ζ is $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

   (a) Show that K is a Galois extension of $\mathbb{Q}$.
   (b) Show that for each integer t, $1 \leq t \leq 6$, there is a *unique* automorphism σ_t of K such that $\sigma_t(\zeta) = \zeta^t$.
   (c) Identify the Galois group of K over $\mathbb{Q}$.

3. Decide whether each of the following statements is true. Justify your answers.

   (a) If R is a commutative ring and I is an ideal of R such that R/I is an integral domain, then R must be an integral domain.
   (b) If R is an integral domain and I is an ideal in R, then R/I is an integral domain.
   (c) If R and S are integral domains, then $R \oplus S$ is an integral domain.

4. Let M be an $n \times n$ matrix with complex entries, and let $V = \mathbb{C}^n$. Suppose that the minimal polynomial of M is $(x-1)(x-2)(x-3)$. Let $p_1(x) = (x-2)(x-3)$, $p_2(x) = (x-1)(x-3)$, $p_3(x) = (x-1)(x-2)$. Note that the greatest common divisor of p_1, p_2, and p_3 is 1, so that one can find polynomials q_1, q_2, q_3 in $\mathbb{C}[x]$ such that $q_1(x)p_1(x) + q_2(x)p_2(x) + q_3(x)p_3(x) = 1$. Let $A_k = q_k(M)p_k(M)$ for $k = 1, 2, 3$.

   (a) Show that
      - $A_1A_2 = A_1A_3 = A_2A_3 = O$ (where O is the $n \times n$ 0-matrix);
      - $A_1 + A_2 + A_3 = I$, where I is the $n \times n$ identity matrix; and
      - $A_k^2 = A_k$ for $k = 1, 2, 3$.

   (b) Let V_k be the range of A_k for $k = 1, 2, 3$. Show that $V = V_1 \oplus V_2 \oplus V_3$.
   (c) Show that $V_k = \ker(M - kI)$ for $k = 1, 2, 3$.

5. Let G be a nontrivial p-group, i.e. $|G| = p^n$, where p is a prime number and $n \geq 1$.

   (a) Show that the center of G is nontrivial.
   (b) Let M be a maximal subgroup of G (so $M \neq G$ and there are no subgroups of G properly between M and G). Show that $[G : M] = p$.
   (c) Show that a maximal subgroup of G is normal in G.

6. Let τ be an automorphism of the real numbers $\mathbb{R}$.

   (a) Show that τ fixes $\mathbb{Q}$.
   (b) Show that $\tau(x) > 0$ if $x > 0$.
   (c) Show that τ is the identity automorphism, i.e. $\tau(x) = x$ for all $x \in \mathbb{R}$.

Pg. 2
Sp. 02

CODE NAME :

[6]. Let F be a finite field with q elements and $a \in F^{\times}$. Assume that $q \equiv 1 \pmod{3}$. Show that $X^3 - a$ is irreducible over F if and only if $a^{\frac{q-1}{3}} \neq 1$.

Algebra
Sp 02
Pg 3

CODE NAME :

[3]. Let

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

(a). Find the characteristic polynomial and the minimal polynomial of A.
(b). Find all eigenvalues for A.
(c). For each eigenvalue λ, find a basis for the corresponding eigenspace.
(d). Is A diagonalizable? Justify.

Page 3
Sp. 02

CODE NAME :

[2]. Let a, b be 5-cycles defined by

$$a = (12345), b = (13524).$$

(i). Show that the centralizer of a in S_5 is the cyclic group generated by a.
(ii). Show that a and b are not conjugate in A_5.

Pg 5
Sp02

CODE NAME :

[5]. Let K be the splitting field of $X^4 - 3$ over $\mathbf{Q}$.
(a). Determine the Galois group of $K/\mathbf{Q}$.
(b). Determine all the quadratic subfields of K over $\mathbf{Q}$ and their corresponding subgroups under the Galois correspondence.
(c). Find all subfields F of K such that $[F : \mathbf{Q}] = 4$ and F is Galois over $\mathbf{Q}$.

Pg 4
Sp 02

CODE NAME :

[4]. For each pair of rings from the list below, decide which are isomorphic. Give a brief justification for your answer. In this problem $M_k(R)$ is the ring of $k \times k$ matrices over the ring R, and $\mathbb{Z}_n$ is the ring of integers mod n.
(a). $M_2(F)$, where F is the field with 4 elements.
(b). $M_2(\mathbb{Z}_4)$.
(c). $\mathbb{Z}_{16} \oplus \mathbb{Z}_{16}$.
(d). $\mathbb{Z}_4 \oplus \mathbb{Z}_{64}$.

Algebra Qualifying Exam Fall 2001

1. Let N be a non-identity normal subgroup of a finite p-group P. Show that $N \cap Z(P) \neq 1$. (Here $Z(P)$ is the center of P.)

2. Let $\mathbb{Q}$ be the rational numbers.

   (a) Prove that $\mathbb{Q}[X]/(X-a)\mathbb{Q}[X]$ is isomorphic to $\mathbb{Q}$ for any $a \in \mathbb{Q}$.

   (b) Suppose that I is an ideal of $\mathbb{Q}[X]$ such that $\mathbb{Q}[X]/I \simeq \mathbb{Q}$. Show that $I = (X-a)\mathbb{Q}[X]$ for some $a \in \mathbb{Q}$.

3. Let $A = \begin{pmatrix} 3 & 1 & 1 \\ 0 & 2 & -1 \\ 0 & 1 & 4 \end{pmatrix}$.

   (a) Determine the characteristic and minimal polynomials of A.

   (b) Let $V = \mathbb{Q}^3$, and let T be the linear transformation from $V \to V$ associated with A. Split V into the direct sum $V = V_1 \oplus V_2 \oplus \cdots$ of cyclic subspaces $V_1, V_2, \ldots$. Find a basis for each V_i.

   (c) Find the Rational Canonical Form (R.C.F) of A.

   (d) Find a matrix P such that $P^{-1}AP$ is in Rational Canonical Form.

4. Let $T : V \to V$ be a linear transformation on a finite dimensional vector space V. Suppose that W_1 and W_2 are eigenspaces of T with distinct eigenvalues λ_1 and λ_2. Let $W = W_1 + W_2$: show that $W = W_1 \oplus W_2$.

5. Let K/F be a Galois extension of fields, of degree n; let p be a prime number dividing n, and write $n = p^k m$ where p does not divide m.

   (a) Show that there is an intermediate field E, $F \subseteq E \subseteq K$, such that E has degree m over F.

   (b) Suppose that E is Galois over F: show that E is then the *unique* extension of F in K of degree m.

6. Let $f(X)$ be the polynomial $X^p - X - 1 \in \mathbf{F}_p[X]$, and let k be the splitting field of f; here p is a prime and $\mathbf{F}_p$ is the finite field with p elements. Let $\sigma(x) = x^p$ (for $x \in k$) be the Frobenius automorphism of k.

   (a) Fix a root α of $f(X)$ in k. Show that $\{\alpha, \alpha+1, \ldots, \alpha+p-1\}$ are all the roots of $f(X)$.

   (b) Show that $k = \mathbf{F}_p(\alpha)$.

   (c) What is the order of σ? *Hint: which root of $f(X)$ is $\sigma(\alpha)$?*

   (d) Show that $f(X)$ is irreducible.

Qualifying Exam in Algebra
March 28, 2001

(Paul Ponomarev, Ombudsperson)

1. Let G be a group, H and K normal subgroups of G.
   a) Prove that there is a homomorphism $\Phi: G \to G/H \times G/K$ with kernel $H \cap K$.
   b) If G/H and G/K are abelian prove that $G/(H \cap K)$ is abelian.

2. Let G be a finite group and P a Sylow p-subgroup of G. Let K be a subgroup of G which contains $N_G(P)$ (the normalizer of P in G). Prove $N_G(K)=K$.

3. Let **Q** denote the rational numbers, **Z** the integers, and p a prime in **Z**. Let $D=\{q \in \mathbf{Q} \mid q$ can be written in form a/b where p does not divide b$\}$.
   a) Prove that D is a subring of **Q**.
   b) Prove that the principal ideal pD has the property: if $d \in D$ and $d \notin pD$, then d is invertible in D.
   c) Prove that there is a homomorphism from D onto $\mathbf{Z}_p$ with kernel pD.

4. Let $A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$ and denote by **R** the field of real numbers.
   a) Find a vector $v \in \mathbf{R}^4$ such that $\{v, Av, A^2v, A^3v\}$ is a basis for $\mathbf{R}^4$.
   b) With v as above, show that if $p(x) \in \mathbf{R}[x]$ and $p(A)v = 0$ then $\deg p(x) > 3$.
   c) With v as above, find a monic polynomial q(x) of degree 4 with $q(A)v = 0$
   d) For q(x) as in c), show that $q(x) = m_A(x)$, the minimal polynomial of A.

5. a) How many similarity classes are there of 8×8 real matrices A with minimal and characteristic polynomials:
$$m_A(x) = (x-1)^3(x+1)^2; \;\; \mathrm{char}_A(x) = (x-1)^5(x+1)^3\,?$$
   b) List a representative for each class listed in part a).

6. Suppose **Q** is the field of rational numbers and K is the splitting field over **Q** of $x^{12}-1$.
   a) Prove that $K = \mathbf{Q}[\sqrt{3}, i]$
   b) Describe the Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$.
   c) List all the subgroups of G and the corresponding subfields of K under the Galois correspondence.

Algebra AU 2001

1. Let G be finite group and p a prime dividing the order of G. Assume that a Sylow p subgroup P of G is cyclic.
5 (i). Show that P has a unique subgroup of order p.
5 (ii). Suppose $P \cap x^{-1}Px \neq \{1\}$ for all $x \in G$. Prove that G possesses a (nonidentity) normal p subgroup.

2. Let Q^+ be the additive group of rational numbers.
5 (i). Let M be a maximal subgroup (assuming it exists) of Q^+. Show that Q^+/M is a group of prime order.
5 (ii). Use (i) to show that Q^+ does not possess maximal subgroups.

3. Let V and W be vector spaces over a field F, and $T : V \to W$ a linear transformation. Let $\{v_1, v_2, \ldots, v_m\}$ be a basis of V. Prove or disprove the following statements :
5 (i). T is surjective if and only if $T(v_1), T(v_2), \ldots, T(v_m)$ span W.
5 (ii). If $T(v_i) \neq 0$ for all $i = 1, 2, \ldots, m$, then the kernel of T is $\{0\}$.

4. Let $M_n(C)$ denote the ring of $n \times n$ matrices with complex entries, $C[X]$ the ring of all polynomials with complex coefficients, and let

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

Let $\phi : C[X] \to M_n(C)$ be the unique ring homomorphism for which $\phi(X) = A$ and $\phi(\alpha) = \alpha$ I for all $\alpha \in C$.
3 (i). Find the characteristic polynomial of A.
4 (ii). Describe explicitly Ker ϕ.
3 (iii). What is the dimension of the image of ϕ as vecter space over C. (Briefly justify).

5. Let Q be the field of rational numbers.
4 (i). Let $K = Q(\sqrt[3]{2})$. Show that $\text{Aut}(K) = \{1\}$.
3+3 = 6 (ii). Find an extension $L \subset C$ of K such that $\text{Aut}(L) \neq \{1\}$ and the degree $[L : K]$ is as small as posssible. Is L uniquely determined ?

6. Let F_p be a field of p elements.
5 (i). Show that there is an irreducible polynomial of degree 2 over F_p.
3 (ii). Find (explicitly) an irreducible polynomial of degree 2 over F_3.
2 (iii). Use (ii) to construct a field of 9 elements.

Sp 2000 Algebra

1. Let G' be the subgroup of a group G generated by all the elements of the form $aba^{-1}b^{-1}$, $a, b \in G$. Prove the following:

4 (a) G' is a normal subgroup of G.

4 (b) G/G' is abelian.

2 (c) Let N be a normal subgroup of G such that G/N is abelian. Then $G' \subseteq N$.

$10 = 4 \times 2\frac{1}{2}$ 2. TRUE or FALSE. Do only 4 of the following, but you need to briefly justify your answers.

(1) Every group of order 60 has a homomorphic image of order different from 60 and 1.

(2) There are 5 non-isomorphic abelian groups of order p^4, p a prime number.

(3) There are no simple groups of order 42.

(4) If a, b are elements of a finite group, then ab and ba have the same order.

(5) If every subgroup of a finite group is normal, then the group is abelian.

3. For each group G with $|G| \leq 4$, find a galois extension field K of the rationals $\mathbb{Q}$ with the Galois group of K over $\mathbb{Q}$ isomorphic to G.

$2\frac{1}{2}$ each for $G \cong C_2$, $G \cong C_3$, $G \cong C_4$, $G \cong C_2 \times C_2$

4. Let K be an extension field of finite degree n over a field F.

3 (a) Let $f(x) \in F[x]$ be the irreducible polynomial for some $\alpha \in K$. Prove that the degree of $f(x)$ divides n.

4 (b) If M is a subring of K and $F \subseteq M \subseteq K$, show that M is a field.

3 (c) Let $\alpha, \beta \in K$ and let $[F(\alpha) : F] = \ell$ and $[F(\beta) : F] = m$, where ℓ and m are relatively prime. Show that $[F(\alpha, \beta) : F] = \ell m$.

5. Let $f(x), g(x) \in \mathbb{Z}[x]$.

6 (a) Suppose $f(x) = g(x)h(x)$. Prove that if a prime number p divides $f(x)$, i.e., p divides every coefficient of $f(x)$, then either p divides $g(x)$ or p divides $h(x)$.

3 (b) If $f(x) \in \mathbb{Z}[x]$ is reducible in $\mathbb{Q}[x]$ then it is reducible in $\mathbb{Z}[x]$.

1 (c) Give an example of a polynomial with degree ≥ 1 which shows that the converse of part (b) is not true.

2 6. (a) State the Cayley-Hamilton theorem.

4 (b) Let A be an $n \times n$ matrix over the field $\mathbb{C}$ of complex numbers. If $Tr(A^i) = 0$ for all $i \in \{1, 2, \ldots\}$, then prove that A has 0 as an eigenvalue.

4 (c) Let A be a 3×3 matrix over the field $\mathbb{C}$ of complex numbers. Suppose $Tr(A) = Tr(A^2) = Tr(A^3) = 0$. Prove $A^3 = 0$.

 2

OCT 06 1999

[1]. Let G be a finite abelian group and a, b be elements of G.
(a). Show that if $\gcd(|a|, |b|) = 1$, then $|ab| = |a||b|$.
(b). Show that there exists an element $g \in G$ of order $\operatorname{lcm}(|a|, |b|)$.

[2]. Let G be finite group with a unique maximal subgroup. Show that G is a cyclic p group.

[3]. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.
(a). Show that $[K : \mathbb{Q}] = 4$ and that $K = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.
(b). Find the minimal polynomial of $\sqrt{3} + \sqrt{5}$ in $\mathbb{Q}[x]$.
(c). List, (need not justify), all the automorphisms of K.
(d). Give, (need not justify), a primitive element for each of the extensions $F/\mathbb{Q}$ such that F is a subfield of K.

[4]. Answer 'true' or 'false'. Briefly justify your answer.
(a). If $K \subset F \subset L$ is a tower of fields such that F/K and L/F are Galois extensions, then L/K is a Galois extension.
(b). If $[F(\alpha), F]$ is odd, then $F(\alpha) = F(\alpha^2)$.
(c). Every element of a field K with p^n elements is a p-th power of some element of K.

[5]. Let R be a ring with 1 and A be a subgroup of the additive group R^+ of R.
(a). Show that the quotient group R^+/A is a ring under the natural product $(a + A)(b + A) = ab + A$ if and only if A is an ideal.
(b). Suppose R is a field and A is an ideal. List all possible structures of the ring R/A.

[6]. Suppose that T is a linear transformation of a vector space $V = \mathbb{R}^5$ with matrix

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

relative to a basis $v_1, \ldots, v_5$. For any $v \in V$ define $m_v(x)$ to be the monic polynomial of least degree such that $m_v(T)(v) = 0$.
(a). Find a vector $w \in V$ such that $m_w(x) = (x-1)^2$.
(b). Find a vector $u \in V$ such that $m_u(x) = (x-1)(x-2)$.
(c). Prove that there is no $w \in V$ such that $m_w(x) = (x-1)^3$.

Spring 99

Algebra Qualifying EXAM

(1). Let K be a normal p-subgroup of a finite group G. Show that K is contained in every Sylow p-subgroup of G.

(2). Let N be a normal subgroup of a finite group G and H be a subgroup of G. Suppose $\gcd(|G:N|, |H|) = 1$. Show that H is contained in N.

(3). Let $S = \mathbb{Q}[x]/x^2\mathbb{Q}[x]$.
(a). Find a basis for S as a vector space over the rational number field $\mathbb{Q}$. Justify.
(b). Which elements of S are units ?
(c). List all the ideals of S.
(d). Prove that there is a nontrivial ring homomorphism from S to the complex number field $\mathbb{C}$.

(4). Suppose that A is an $n \times n$ matrix over the complex number field $\mathbb{C}$ and $A^m = 0$ for some $m > 0$.
(a). Show that if λ is an eigenvalue of A,then $\lambda = 0$.
(b). Determine the characteristic polynomial of A.
(c). Prove $A^n = 0$.
(d). Write down a 5×5 matrix B for which $B^3 = 0$ but $B^2 \neq 0$.
(e). If M is any 5×5 matrix over $\mathbb{C}$ with $M^3 = 0$ and $M^2 \neq 0$, must M be similar to the matrix B in part (c) ? Justify your answer.

(5). (a). Find the degree of the extension $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ over $\mathbb{Q}$.
(b). Find an element u in K such that that $K = \mathbb{Q}(u)$. Justify your answer.

(6). Let $K = \mathbb{Q}(\sqrt{3+\sqrt{5}})$.
(a). Show that K is a splitting field of $X^4 - 6X^2 + 4$.
(b). Find the structure of the Galois group of $K/\mathbb{Q}$.

4

Qualifying Exam in Algebra

September 21, 1998

1. Which pairs of groups from the following list are isomorphic. Justify your answer. Here S_3 denotes the symmetric group on three letters; C_n denotes the cyclic group of order n.

(a) $C_2 \times C_{18}$ (b) $C_4 \times C_9$ (c) $C_6 \times S_3$ (d) $S_3 \times S_3$

2. Suppose G is a group.

(a) Use the class equation to prove that if $|G| = 9$ then G is abelian.

(b) If $|G| = 45$ prove that G is abelian.

3. Let A be a commutative ring with 1. An element $c \in A$ is said to be <u>nilpotent</u> if: $c^n = 0$ for some $n \geq 1$. Let N be the set of all nilpotent elements of A.

(a) Prove that N is an ideal of A.

(b) Prove that A/N has no nonzero nilpotent elements.

(c) If $x \in N$ show that $1 - x$ and $1 + x$ are units in A.

4. (a) Show that the splitting field F of the polynomial $x^{12} - 1$ over the field Q of rational numbers equals $Q(\sqrt{-1}, \omega)$, where ω is a primitive cube root of 1.

(b) List the elements of the Galois group $G = G(F/Q)$.

(c) List all subgroups of G and all subfields of F.

(d) Write out the one to one Galois correspondence between these two lists.

5. Determine whether or not $\sqrt{-1}$ is in the field $Q(\alpha)$ where $\alpha^3 + \alpha + 1 = 0$. Justify your answer.

6. Let V be a finite dimensional vector space over the field C of complex numbers

(a) Suppose $S, T \in \mathrm{End}_C(V)$ with $ST = TS$. Show that there exists $v \in V$ which is an eigenvector for <u>both</u> S and T.

(b) Let R be a subspace of $\mathrm{End}_C(V)$ of pairwise commuting transformations. Use part (a) to show that there exists a nonzero vector v which is an eigenvector for <u>every</u> element of R.

(c) Let G be an infinite subset of pairwise commuting transformations in $\mathrm{End}_C(V)$. Show that there exists a common eigenvector for G. That is, there exists a nonzero vector v which is an eigenvector for <u>every</u> element of G.

Qualifying Exam in Algebra

April 1, 1998

1. (a) If $f : G_1 \to G_2$ is an isomorphism of groups, prove:

$$G_1 \text{ is abelian if and only if } G_2 \text{ is abelian.}$$

(b) Show that there exist two non-isomorphic groups of order $2k$, provided $k > 1$.

2. Suppose S a Sylow p-subgroup of a finite group G, and N the normalizer of S in G. Suppose H is a subgroup of G and $g \in G$. If H contains N and gNg^{-1}, prove that $g \in H$.
(Hint: Prove that S and gSg^{-1} are Sylow subgroups of H. Apply the Sylow Theorem for H.)

3. Prove that a linear transformation $F : V \to V$ of a finite dimensional vector space V is nilpotent if and only if there is a basis of V in which the matrix for T is triangular with all diagonal entries zero.

4. Let G be a finite group and F a field. Suppose R is a vector space over F with basis $\{e_g : g \in G\}$. For two elements $u = \sum_{g \in G} x_g e_g$ and $v = \sum_{g \in G} y_g e_g$ in R, with $x_g, y_g \in F$, define their product to be:

$$u \cdot v = \sum_{g,h \in G} x_g y_h e_{gh}$$

In particular, $e_g \cdot e_h = e_{gh}$ for any $g, h \in G$. You may assume that R is a ring.
Let $u_0 = \sum_{g \in G} e_g$. Prove that the 1-dimensional subspace $I = F \cdot u_0$ is a two-sided ideal of R.

(over)

5. Let $f_k(x) = x^{1999} + 1998x + k$, where k is an integer. Let Q be the field of rational numbers.

(a) Show that there exist infinitely many integers k such that $f_k(x)$ is irreducible in $Q[x]$.

(b) Show that there exist infinitely many integers k such that $f_k(x)$ is reducible in $Q[x]$.

(Hint : When can an integer n be a root of the polynomial $x^{1999} + 1998x + k$?)

6. Suppose K is a subfield of C, the field of complex numbers, and K admits no proper odd degree extension. That is, if E/K is an extension field of odd finite degree then $E = K$.

(a) If F/K is a finite Galois extension, prove that $[F : K] = 2^m$ for some m.

(b) If L/K is an extension field of finite degree, prove that $[L : K] = 2^n$ for some n.

(Hints. (a) Sylow subgroups may be relevant here.
(b) It might be reasonable to use part (a) in the proof.)

Qualifying Exam in Algebra

September 22, 1997

1. (a) Let F_2 be the field of 2 elements. Express the polynomial $f(x) = x^5 + x^4 + 1$ as a product of irreducible factors in $F_2[x]$.

(b) Let K be the splitting field of f(x) over F_2, Find $[K: F_2]$. Describe $Gal(K/F_2)$.

(c) How many subfields does K have? Justify your answer.

2. Answer "True" or "False" to each question. Briefly justify your answers.

(a) Up to isomorphism there is exactly one field with 36 elements.

(b) If K/F is a field extension such that $[K : F] = n$ and if $(m, n) = 1$, then an irreducible polynomial of degree m in F[x] has no roots in K.

(c) If $F \subset K \subset L$ is a tower of fields such that K/F and L/K are Galois extensions, then L/F is a Galois extension.

(d) Let **C** and **Q** denote the fields of complex and rational numbers. Suppose $\eta \in \mathbf{C}$ with $\eta^5 = 1$. Then -1 is not a sum of squares in the field $\mathbf{Q}(\sqrt[5]{2}\cdot\eta)$

[Hint. Recall that $x^5 - 2$ is irreducible in $\mathbf{Q}[x]$, and the field $\mathbf{Q}(\sqrt[5]{2})$ is contained in the field of real numbers.]

3. Let $v_1 = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}$, $v_2 = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}$, $v_3 = \begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}$ in $\mathbf{R}^3$.

(a) Prove that $\{ v_1, v_2, v_3 \}$ is a basis for $\mathbf{R}^3$

(b) Suppose that $T: \mathbf{R}^3 \to \mathbf{R}^3$ is a linear transformation such that

$$T(v_1) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad T(v_2) = \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix}, \quad T(v_3) = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}.$$

Find $T(\begin{bmatrix} 2 \\ 1 \\ -2 \end{bmatrix})$.

(c) Find the matrix of T with respect to the basis $\{v_1, v_2, v_3\}$.

Qual ? alg. 8 Au 94

4. Suppose G is a finite group. The notation $H \trianglelefteq G$ means: H is a normal subgroup of G. A subgroup $A \subseteq G$ is "characteristic" if: $\varphi(A) \subseteq A$ for every automorphism $\varphi : G \to G$. In this case we write $A \text{ char } G$.
   (a) If $A \text{ char } H$ and $H \trianglelefteq G$ prove that $A \trianglelefteq G$.
   (b) Prove that $Z(G) \text{ char } G$, where $Z(G)$ is the center of G.
   (c) Suppose p is a prime and a Sylow p-subgroup S of G happens to be normal $(S \trianglelefteq G)$. Prove: $S \text{ char } G$.

5. Let $G = GL(2, p)$ be the group of all invertible 2×2 matrices over the field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.
   (a) If $g_a = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ for $a \in \mathbf{F}_p$ show that $g_a^p = 1$.
   (b) If $h \in G$ is an element of order p prove that h must be conjugate to $g_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
   That is: $h = s \cdot g_1 \cdot s^{-1}$ for some $s \in G$.
   (Hint. Canonical form theory might help here. Determine the minimal polynomial $m_h(x) \in \mathbf{F}_p[x]$.)

6. (a) If the ring R is a P.I.D. prove that every non zero prime ideal in R is maximal.
   (b) In the ring $\mathbf{Z}[x]$ (where $\mathbf{Z}$ denotes the ring of integers), prove that the ideal (x) is a prime ideal which is not maximal.

9

Qualifying Exam in Algebra April 2,1997

There are six questions.Answer each question on a separate sheet(s) of paper provided. Be sure to put your code name on each sheet of paper you wish to be graded. GOOD LUCK!

1. a) Complete the following statement, (Need not justify) ;
   A non-empty subset N of a group G is a normal subgroup if and only if .... (2)
   b) For a group G , let $Z(G) = \{ z / z \in G , z g = g z$ for all $g \in G \}$
   Show that Z(G) is a normal subgroup of G (6)
   c) For $G = S_3$ the Symmetric group of degree 3 , list (need not justify), the normal subgroups. What is Z(G) ? Justify. (2)

2. a) Give the definition of a simple group. (3)
   b) Show that there are no simple groups of order 42. (4)
   c) For $n > 4$, what are the possible orders of homomorphic images of A_n, the alternating group? Briefly justify this statement. (3)

3. Let $R = Z[i] = \{ a + b i / a , b \in Z \}$ be the principal ideal domain of Gaussian Integers. Let (α) denote the principal ideal generated by α.
   a) Show that (13) is not a prime ideal of R. (3)
   b) The quotient ring R / (13) is not a field. Justify this statement. (4)
   c) Give an ideal I of R different from (13) and R which contains (13) and show that R/I is a field. (3)

4. Let M be an nxn matrix over a field F and let $p_M(x) \in F[x]$ be its characteristic polynomial. Assume $p_M(x) = (x - \lambda_1)(x - \lambda_2).......(x - \lambda_n)$ where $\lambda_i \in F$ are not necessarily distinct. Show
   a) The matrix M is similar to a triangular matrix T. Briefly justify this statement. (3)
   b) If $g(x) = b_0 + b_1 x+.....b_m x^m \in F[x]$, prove that the characteristic polynomial for the matrix g(M) is exactly (4)
   $(x - g(\lambda_1))(x - g(\lambda_2))......(x - g(\lambda_m))$
   (HINT : Use part (a))
   c) If g(x) and $p_M(x)$ are relatively prime in F[x], explain why g(M) must be a non-singular matrix (3)

/10

5. Let Q denote the field of rational numbers.

a) Show that the polynomial $f(x) = x^4 - 2$ is irreducible in Q[x]. (3)

b) What is the degree $[\,Q(\alpha) : Q\,]$ where α is a root of $x^4 - 2$? Justify. (4)

c) Write $\dfrac{1}{\alpha^3 + 2}$ in the form $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$, $a_i \in Q$. (3)

6. Let Q denote the field of rational numbers.
Answer "True" or "False". Briefly justify your answers.

a) For every positive integer n there exists an extension E of Q such that [E:Q] = n, (2)

b) Every irreducible polynomial of degree n in Q[x] has n distinct roots in an extension field. (2)

c) The fields $Q(\sqrt[3]{2})$, $Q(\sqrt[3]{2}\,\omega)$ are isomorphic where ω is a primitive cube root of unity. (2)

d) The fields $Q(\sqrt{2})$ and $Q(\sqrt{3})$ are isomorphic. (2)

e) A finite extension E/F of a finite field F has a cyclic Galois group. (2)

11

Au 96

Qualifying Exam in Algebra

September 23, 1996

1. Show that there does not exist any simple group of order 56.

2. Show that there are precisely 2 non-isomorphic non-abelian groups of order 8.

3. Let Q denote the field of rational numbers and let S be the set of all polynomials $f(x)$ in $Q[x]$ such that some power of $f(x)$ is divisible by $(x^2+5)^3 \cdot (x+2)^2$ in $Q[x]$

(a) Show that S is an ideal in $Q[x]$.

(b) Find a polynomial of least degree in S.

4. Let R be the field of real numbers and let U be the subspace of R^3 spanned by $\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix}$. Find an orthonormal basis for R^3 which contains a basis of U.

5. Suppose that A is a 5×5 complex matrix with exactly two eigenvalues, -1 and 2, and suppose that the dimension of the 2-eigenspace is 3, that is: $\dim(\ker(A - 2 \cdot I)) = 3$.

(a) What are the possible Jordan Canonical Forms for A? Explain briefly why your list is complete.

(b) For each Jordan Canonical Form listed in (a), write down the Rational Canonical Form, the minimum polynomial and the characteristic polynomial.

6. Suppose Q is the field of rational numbers and K is the splitting field over Q of $x^8 - 1$.

(a) Find $[K : Q]$.

(b) Describe the Galois group $G = \mathrm{Gal}(K/Q)$.

(c) List all the subgroups of G and the corresponding subfields of K under the Galois correspondence.

SP 96 12

Qualifying Exam in Algebra
March 25, 1996

(H. Allen, Ombudsperson)

1. Let $GL(2, \mathbb{C})$ denote the group of all 2×2 invertible matrices with complex entries and let $SL(2, \mathbb{C})$ denote the subgroup of $GL(2, \mathbb{C})$ consisting of matrices of determinant 1.
   (a) Determine all the elements of $SL(2, \mathbb{C})$ of order 2. Justify your conclusion.
   (b) Give an example of an element A of $GL(2, \mathbb{C})$ with $A^2 = 1$ but $A \neq \pm I$.

2. If G is a finite group of order 36, prove that G has a normal subgroup of order either 3 or 9.

3. (a) Suppose R is a ring with identity 1. Suppose $x \in R$, n is a positive integer, and $x^n = 0$. Prove that $x + 1$ is a unit in R.
   (b) Suppose R is a ring with identity $1 \neq 0$. Prove that R is a division ring if and only if R has no left ideals other than R and 0.

4. Suppose K/F is an algebraic extension of fields (allowing the possibility that $[K : F]$ is infinite). Either prove the following statement or find a counterexample:

   If R is a subring of K with $F \subseteq R \subseteq K$, then R must be a field.

5. Suppose K is a field with a finite number of elements.
Prove that $|K| = p^n$ for some prime number p and some positive integer n.

6. Let $A = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$.
   (a) Find an invertible matrix P so that $P^{-1}AP$ is a diagonal matrix.
(Hint: Note that $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ is an eigenvector of A.)
   (b) Find a matrix Q which in orthogonal (i.e. $Q^T = Q^{-1}$) such that $Q^{-1}AQ$ is diagonal.

Au 95

1

Qualifying Exam in Algebra

September 18, 1995

(P. Ponomorev, Ombudsperson)

1. Let A_5 be the alternating group of degree 5.
   (a) Show that A_5 does not contain subgroups of order 15, 20, or 30.
   (b) Show that A_5 contains a subgroup of order 10.

2. Suppose that the matrix $A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$ acts as a linear transformation on $\mathbf{R}^5$ where $\mathbf{R}$ is the field of real numbers.
   (a) Find the characteristic polynomial of the resulting linear transformation.
   (b) Find the minimal polynomial of the resulting linear transformation.
   (c) Find a basis for the eigenspace corresponding to eigenvalue 1.
   (d) Find the rational canonical form of A.

3. Let V be a vector space over R (where R is the field of real numbers), v, w non-zero elements in V, and T a linear operator on V. Suppose that $T(v) = 2v$, $T(w) = -w$.
   (a) Prove that v and w are linearly independent. (Do not just quote a theorem here.)
   (b) Prove that $(x+1)(x-2)$ is the monic polynomial $f(x) \in R[x]$ of least degree such that $f(T)(v+w) = 0$.

14

Au95 (7)

4. Suppose R is a ring with identity and define the <u>center</u> Z of R to be

$$Z = \{z \in R : zr = rz \text{ for every } r \in R\}.$$

(1) Prove that Z is a subring of R.

(2) Suppose $e \in Z$ satisfies $e^2 = e$. Define $f = 1 - e$ and prove that $f^2 = f$ and $ef = fe = 0$.

(3) Prove that Re and Rf are 2-sided ideals of R such that $Re \cap Rf = (0)$ and $Re + Rf = R$. Also prove that Re and Rf are rings with identity.

(4) Define $\varphi : R \to (Re) \oplus (Rf)$ by $\varphi(r) = (re, rf)$. Is this map φ a ring isomorphism? Justify your answer.

5. Let F be the splitting field of the polynomial $x^4 - 3$ over the field Q of rational numbers.

3 (a) Find the degree of the extension $[F : Q]$

3 (b) Determine the Galois group G of F/Q.

4 (c) Find all subgroups of G of order 4 and explicitly describe the corresponding subfields.

(*Hint*: There are 3 subgroups of order 4)

6. Let $K = Z_2(\alpha)$ where α is a root of $x^4 + x + 1$ in an extension field of Z_2. (Here Z_2 is the field of two elements, and you may assume that $x^4 + x + 1$ is irreducible in $Z_2[x]$.) Is α a generator of the multiplicative group $K^\#$? Justify your answer.

Original in RED : Don't even THINK about REMOVING!

15

SP 95

Qualifying Exam in Algebra March 27, 1995

(A. Ash, Ombudsperson)

1. Let G be a group of order $495 = 3^2 5.11$. Prove that G has a normal subgroup of order 5 or 11.

2. Let G be a finite group with a normal subgroup H such that G/H is cyclic of order m·n for some m∈N. Prove that G has a normal subgroup K such that [G:K] = n.

3. Let V be a vector space, $S, T \in \mathrm{End}(V)$ with $S \circ T = T \circ S$.
   a) Prove: If V_λ is the λ-eigenspace for S, then $T(V_\lambda) \subseteq V_\lambda$.
   b) Give examples of $S \neq \alpha I$, T with $S \circ T = T \circ S$ and an S-invariant subspace U of V such that $T(U) \not\subset U$.

4. Let $T: R^n \to R^n$ be a nilpotent operator (i.e. $T^k = 0$ for some $k \in N$)
   a) Prove that there exists a basis for R^n with respect to which the matrix of T is lower triangular.
   b) Prove that if T is diagonalizable, then T = 0.
   c) Give an example with n=3 such that T has a unique invariant subspace in each dimension.

5. Let R be a ring, I_1 and I_2 ideals of R such that $I_1 + I_2 = R$. Prove that $R/(I_1 \cap I_2) \cong (R/I_1) \times (R/I_2)$.

6. Let $F_p = Z/pZ$ be the field of p elements, where p is a prime number. Suppose K is an extension field of F_p of degree n (so that K is a field of p^n elements). Let $K^* = K - \{0\}$ and $F_p^* = F_p - \{0\}$ denote the multiplicative groups of units.
   a) If $a \in K^*$, prove that $a^{p-1} = 1$ if and only if $a \in F_p^*$.
   b) If $a \in K^*$, define $N(a) = a^{(p^n-1)/(p-1)}$. Prove that $N(a) \in F_p^*$ and that $N: K^* \to F_p^*$ is a group homomorphism.
   c) Is N necessarily a surjective map?

15 16

Au 94

1

Qualifying Exam in Algebra September 19,1994

(P. Ponomarev Ombudsperson)

I. Suppose that $G = \langle g \rangle$ is a cyclic group of order 35.

(a) Prove (without using Sylow Theory) that G has a subgroup of order 7.

(b) Prove that there is a surjective homomorphism $\varphi : G \to C_5$ where C_5 is a cyclic group of order 5

II. Let G be a group, Aut(G) the set of all automorphisms of G.
Let $\varphi_g : G \to G$ be defined by $\varphi_g(x) = g \cdot x \cdot g^{-1}$.

(a) Prove that φ_g is an automorphism of G.

(b) Prove that the map $\sigma : g \longmapsto \varphi_g$ is a homomorphism from G to Aut(G).

(c) Show that the kernel of σ is the center of G.

III. Let R be a commutative ring with 1. An ideal $M \neq R$ is said to be <u>maximal</u> if : whenever I is an ideal with $M \subseteq I \subseteq R$ then either $I = M$ or $I = R$. Show that M is maximal if and only if the quotient ring R/M is a field.

IV. Let $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -2 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

(a) Detemine the characteristic and minimal polynomials of A.

(b) Find the Jordan Canonical Form of A.

V. Let W be a proper subspace of V with $\dim W \leq \dim V - 2$.

(a) Show that W is the intersection of two proper subspaces.

(b) Is the result in (a) true if one assumes only that W is proper?

A 0 94
A 5 35 2

VI. Suppose $\alpha, \beta \in C$ are algebraic over Q and consider the fields $K = Q(\alpha)$ and $L = Q(\beta)$. (Here Q is the field of rational numbers and C is the field of complex numbers.)

(1) Prove that $[L(\alpha) : L] \leq [Q(\alpha) : Q]$.

For the remaining parts of this problem assume that $Q(\alpha)/Q$ is a Galois extension.

(2) Show that $L(\alpha)/L$ is also a Galois extension.

(3) Let $G = \mathrm{Gal}(Q(\alpha)/Q)$ and $H = \mathrm{Gal}(L(\alpha)/L)$ be the Galois groups. If $h \in H$ let $h|_{Q(\alpha)}$ denote the restriction of h to $Q(\alpha)$. Show that $h|_{Q(\alpha)}$ is an automorphism of $Q(\alpha)$.

(4) Show that the map $\rho : H \to G$ defined by $\rho(h) = h|_{Q(\alpha)}$ is an injective homomorphism of groups.

ORIGINAL -- DO-NOT-Remove! 178

Qualifying Exam in Algebra

March 28, 1994
J. Hsia, Ombudsman

-SP 94

1. Let M, N be normal subgroups of a group G.

   a) Show that $G/(M\cap N)$ is isomorphic to a subgroup of the direct product $G/M \times G/N$.
   b) If $M\cap N = \{1\}$ and G/M and G/N are abelian, show that G is abelian.

2. Let H be a non-trivial proper normal subgroup of a group G, and P a Sylow p-subgroup of H.

   a) Show that $P^g = g^{-1}Pg$ is also a Sylow p-subgroup of H for any g in G
   b) Show that for each $g\in G$, $P^g=P^h$ for some $h\in H$
   c) Show that $G = N_G(P)\cdot H$ where $N_G(P)$ is the normalizer of P in G

3. a) Show that $x^4 - 2$ is irreducible in $Q[x]$
   b) Find the splitting field F of the polynomial $x^4 - 2$ over Q
   c) Find the Galois group $G = G(F/Q)$

4. Let E and F be field extensions of Q (within C) of degrees n and m respectively. Let EF denote the compositum of E and F (i.e. the smallest subfield of C containing both E and F).

   a) Show that $[EF:Q] \leq nm$
   b) Give an example of E, F (E≠F) for which $[EF:Q] < nm$

5. Let A be a real matrix with characteristic polynomial $(x-1)^2(x-2)^3$. If the eigenspace for the eigenvalue 2 is two-dimensional, what are the possible Jordan canonical forms for A? Justify your answer (briefly)

6. Let $A\in M_n(F)$, $m(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ the minimal polynomial of A.

   a) Show that the F-subalgebra of $M_n(F)$ generated by $F\cdot I \cup \{A\}$ is $\mathrm{Span}\{I, A, A^2, \ldots, A^n, \ldots\}$.
   b) Show that $\{I, A, A^2, \ldots, A^{d-1}\}$ is a basis for the F-subalgebra generated by $F\cdot I \cup \{A\}$

Do-NOT Remove ORIGINAL 19 = AU 92

Qualifying Exam in Algebra · September 20,1993

I. (a) If A and B are subgroups of a finite subgroup G satisfying the condition $A \cap B = \{e\}$, then show that $|A \cdot B| = |A| \cdot |B|$ Where $A \cdot B = \{ a.b \,/\, a \in A, b \in B \}$

(b) If G is any finite group of order pq where p, q are primes with $p < q$; then prove that G can not contain two distinct subgroups of order q (Do Not use Sylow theorems).

II. (a) Define <u>Integral Domains</u>.

(b) Prove : Every finite integral domain is a field.

(c) Give an example (no proofs necessary) of a finite integral domain.

III. (a) Let F be a field, $a \in F$, $g(x) \in F[x]$. Prove that a is a root of $g(x) = 0$ if and only if $x - a$ is a factor of $g(x)$.

(b) Prove that if the degree of $g(x)$ is n, then $g(x)$ has at most n distinct roots in F.

IV. (a) Suppose that K/F is a field extension of finite degree $[K:F]=n$. Suppose $f(x) \in F[x]$ is irreducible of degree d and $f(x)$ has a root in K, then prove that $d \mid n$.

(b) Let $GF(q)$ denote the finite field consisting of q elements. Is $x^3 + 2x + 1$ irreducible in $GF(81)$? Explain.

V. Let $A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

a. Compute the characteristic and the minimal polynomials for A.

b. What is the Jordan canonical form of A ?

c. What is the rational canonical form of A ?

VI. Let A be an $m \times n$ matrix with coefficients in a field F, prove that if A has a left inverse i.e. there exists an $n \times m$ matrix B such that $BA = I_n$, then the columns of A are linearly independent.

Qualifying Exam in Algebra

April 1, 1993
M. Madan ombudsman

-Sp 93

1. (a) Find an element of maximal order in S_7.
   (b) Find an element of maximal order in A_7.

2. Let G be a group, $a,b \in G$ with $ab = ba$. If $\gcd(|a|,|b|) = 1$, prove that $|ab| = |a||b|$. ($|g|$ denoting the order of g).

3. Find an orthogonal matrix P with PAP^t diagonal for $A = \begin{pmatrix} 2 & 1 & -2 \\ 1 & 2 & 2 \\ -2 & 2 & -1 \end{pmatrix}$.

4 Let F be a field, $\{0\} \neq I \subseteq F[x]$ an ideal. Prove that $\exists$ a monic polynomial $d(x) \in I$ such that for all polynomials $p(x)$, $p(x) \in I \Leftrightarrow d(x) | p(x)$

5. Prove that if A and B are 3×3 matrices with the same minimum and characteristic polynomials, then A and B are similar. Hint: think rational canonical form.

6. (a) Prove that the polynomial $x^4 + 1$ is irreducible in Q[x].
   (b) Find the degree of the splitting field E of $x^4 + 1$ over Q.
   (c) Describe the Galois group Gal(E/Q)

Qualifying Exam in Algebra

Aug 92

September 23,1992
W. Sinnott ombudsman

I. Let G be a finite group of odd order which acts as a group of permutations on a finite set X of odd cardinality. Prove: The number of G-orbits on X is odd.

II. Let G be a finite group and H a normal subgroup of G with $(|H|,[G:H])=1$.
Prove: If α is an automorphism of G, then $\alpha(H)=H$.

III. Let F be a field and R an integral domain that is also a finite dimensional F-vector space. Show that R is also a field.

IV (a) Show that x^3-2 is irreducible in Q[x].
(b) Find the splitting field F of the polynomial x^3-2 over Q.
(c) Find the Galois group $G=G(F/Q)$.
(d) Find all subgroups of G and all subfields of F and set up a 1 to 1 Galois correspondence between subgroups and corresponding subfields.

V. Let $A=\begin{pmatrix} -13 & 0 & -25 \\ -12 & 2 & -20 \\ 9 & 0 & 17 \end{pmatrix}$

a. Compute the characteristic and minimal polynomials for A.
b. What is the Jordan canonical form of A ?
c. What is the rational canonical form of A ?

VI. Let V be a vector space over the field k, W a subspace of V with basis $\{w_1,w_2,\dots\dots,w_s\}$, $v\in V$ but $v\notin W$. Prove that $\{w_1,w_2,\dots\dots,w_s, v\}$ is a linearly independent subset of V.

Algebra Qualifying Exam Spring 1992

A.Silverberg ombudsperson

Sp 92

Throughout this exam, Z, R, C are the integers, reals and complex numbers, respectively.

1. Define a mapping $\varphi: Z[X] \to C$, by setting $\varphi(f(X)) = f(i)$ where $i = \sqrt{-1}$.
   (a) Verify that φ is a ring homomorphism.
   (b) Suppose $f(X), g(X) \in Z[X]$, $g(X)$ monic with $g(X) \mid f(X)$ in $R[X]$. Show that $g(X) \mid f(X)$ in $Z[X]$
   (c) Verify that $\ker(\varphi) = (X^2 + 1)$, the (principal) ideal in $Z[X]$ generated by $X^2 + 1$.
   (d) Verify that $X^2 + 1$ is irreducible in $Z[X]$.

2. Let $V = R^4$ equipped with the standard inner product. Let W be the subspace spanned by the vectors $\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} -1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$. Find a basis for $W^{\perp} \subseteq R^4$.

3. Consider the 3×3 matrix $A = \begin{bmatrix} 2 & a & c \\ 0 & 2 & b \\ 0 & 0 & 2 \end{bmatrix}$ where a, b, c are real numbers.
   a. Show that A is diagonalizable $\Leftrightarrow$ $a=b=c=0$.
   b. Show that A has at least two linearly independent eigenvectors $\Leftrightarrow$ $ab=0$.
   c. Find two linearly independent eigenvectors for A if $a=c=1$ and $b=0$.

4. Let $0,1 \neq a \in Z$ be fixed. Set $S = \{s \in Z \mid \gcd(a,s) = 1\}$.
   (a) Show that S is closed under multiplication with $0 \notin S$.
   (b) Let $M = \{(r,s) \mid r \in Z, s \in S\}$ and define $(r,s) \sim (r',s')$ if $rs' = sr'$. Show that $\sim$ is an equivalence relation.
   (c) Let $[r,s]$ denote the class of (r,s) in $(M,\sim)$ and Z_S the set of all equivalence classes. It is known that $[r,s] + [r^*,s^*] = [rs^* + sr^*, ss^*]$ and $[r,s]\cdot[r^*,s^*] = [rr^*, ss^*]$ equip Z_S with the structure of a commutative ring with identity. Determine the additive identity and the multiplicative identity in Z_S.
   (d) Define $\varphi: Z \to Z_S$ by setting $\varphi(x) = [x,1]$. Show that φ is a homomorphism of rings with identity and determine $\ker(\varphi)$.
   (e) For $s \in S$, verify that $\varphi(s)$ has a multiplicative inverse in Z_S.

5. Let F be a finite field.
   ✓ (a) Show that there is a prime p with $|F| = p^e$ for some $e \geq 1$.
   (b) Show that $x^{p^e - 1} = 1$ for all $x \in F^*$, the set of all non-zero elements of F.

6. Let G be a cyclic group of order n. Prove that every subgroup of G is cyclic.

Qualifying Examination in Algebra January 8, 1992

W 92

(1) Let p be a prime in Z and let I be the set of all polynomials in Z[x] which have a constant term divisible by p. Show the following:

(a) I is an ideal of Z[x]

(b) I is maximal

(c) I is not principal

(d) Z[x]/I is isomorphic to Z_p.

2. Let E be the set of even integers with ordinary addition but with a new multiplication $*$ defined by $a * b = ab/2$ where the right hand side is ordinary multiplication in Z. Prove

(a) E is a commutative ring with identity

(b) The map $f: E \to Z$ given by $f(x) = x/2$ is an isomorphism.

3. If V is a finite dimensional inner product space with a subspace W, prove that V is the direct sum of W and $W^{\perp}$.

4. Determine an orthogonal matrix P such that $P^T \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix} P$ is diagonal.

5. If G is a nontrivial finite p-group (i.e. $|G| = p^n$, $n \geq 1$, where p is a prime) then show that the center of G is nontrivial.

✓6. If F is any finite field then show that F^*, the set of nonzero elements of F, forms a cyclic group under the field multiplication.

Qualifying Exam in Algebra **October 2,1991**

1. Show that any group of order 224 contains a subgroup of order 28.

2. Let x be an element of a group G with order of $x = mn$, where m and n are relatively prime integers. Show that there are unique elements a and b in G such that $x = a . b = b . a$ and order of $a = m$, and order of $b = n$.

3. Find the splitting field of the polynomial $x^3 - 2$ over Q the field of rationals. Also find its Galois group G. Find all subgroups of G and the corresponding fixed fields in the Galois correspondence and set up a one to one correspondence between them.

4. Construct an explicit isomorphism between the following two finite fields:

$$F_1 = Z_3[x] / x^3 + 2x + 2 \quad \text{and } F_2 = Z_3[x] / x^3 + x^2 + 2 .$$

Hint: $a = x^2 + x + 1$ is a root of $y^3 + 2y + 2$ in F_2 .

5. Show that every mxn matrix of rank 1 over the reals has the form $X.Y^T$ where X,Y are column matrices.

6. Let S, T : $C^n \to C^n$ be linear transformations such that ST=TS Show that if T is diagonalizable then S maps any eigenspace of T into itself.

7. Let R be the reals and let T be the ring of continuous functions from R to R.

a. Show that if f in T is such that $f^3 = f$ then then f is one of three constant functions.

b. Show that T is not isomorphic to R x R

8. Let a,b be in Z and let (a,b) denote the g.c.d. of a ,b and [a,b] denote the l.c.m. of a,b . Show there exists divisors u of a and v of b such that (u,v)=1 and u.v=[a,b]

PhD Qualifier W91 ①

Algebra ~~Proficiency~~ Examination 1/9/91

There are six questions. Answer each question on a separate sheet(s) of paper provided . Be sure to put your code name on each sheet of paper you wish to be graded. Do not use any theorem which reduces the stated problem to a triviality.
Throughout, Z denotes the rational integers and Q the field of rational numbers.

1. Suppose G is a group and $g \in G$ has finite order n. Prove the following statements:

(i) If k is an integer relatively prime to n then g^k also has order n.

(ii) If d is a positive integer dividing n then g^d has order n/d.

2. Let S be a set of prime numbers and define $\Pi(S)$ to be the set of all finite products of elements of S (with repetitions allowed). Include 1 in $\Pi(S)$ as the "empty product".

For example, if $S = \{2\}$ then $\Pi(S) = \{1,2,4,8,...\}$.

Define $R_S = \{m/n : m,n \in Z \text{ and } n \in \Pi(S)\}$, the set of all fractions with denominators in $\Pi(S)$. Clearly, $Z \subseteq R_S \subseteq Q$. Answer the following:

(i) If $a/b \in Q$ where $a,b \in Z$ and a,b are relatively prime and $b>0$ then prove: $a/b \in R_S$ if and only if $b \in \Pi(S)$.

(ii) Prove R_S is a subring of Q.

(iii) If T is another set of prime numbers , is it true that

$$R_S \cap R_T = R_{S \cap T} \;?$$ Justify your answer.

✓3. Let F be the field with p^n elements where p is prime and let F^* denote its multiplicative cyclic group of order $p^n - 1$. Answer the following:

✓(i) Show that $\sigma : a \to a^p$ defines an automorphism of F.

(ii) Show that σ is of order n.

✓(iii) Deduce that the group of all automorphisms of F is cyclic of order n.

Algebra Ph.D Qualifier p2 1/9/91

w/91

4. Answer "true" or "false" and briefly justify your answers:

(i) For every positive integer n, Q has an extension of degree n.

(ii) $Q(\sqrt[7]{2}, \sqrt[5]{2})/Q$ is not a simple extension.

(iii) Given a finite group G, there exists some field extension F/K such that Gal(F/K) is isomorphic to G.

(iv) a polynomial f(x) in Q[x] that is irreducible of degree n has exactly n distinct roots in its splitting field over Q.

5. Given $A = \begin{bmatrix} 3 & 1 & 0 & 1 \\ 0 & 3 & 0 & 2 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$

Find the characteristic polynomial, the minimal polynomial, the eigenvalues, eigenvectors and Jordan Form of A. You need not give the basis corresponding to the Jordan Form.

6. Suppose V is a vector space of unknown dimension n over Q. Let $T : V \to V$ be a linear transformation with minimal polynomial $x^4 - x^2 - 2$ over Q. Answer the following:

$= (x^2-2)(x^2+1)$

(i) Show that n is even.

(ii) Let $V_1 = \{v \text{ in } V : T^2v = -v\}$ and let $V_2 = \{v \text{ in } V : T^2v = 2v\}$. Show that both V_1 and V_2 are T - invariant and that $V = V_1 \oplus V_2$.

Qualifier SU 90 Algebra 27

Use a separate sheet for each problem attempted. Do not quote any result which would trivialize the problem attempted. A sufficient condition for passing is the complete solution of at least four of the six problems.

1. a. Determine, up to isomorphism, all abelian groups of order 12.

   b. Describe two non-isomorphic non-abelian groups of order 12. Briefly justify your claims that they are non-abelian and non-isomorphic.

2. a. Let p be a prime integer. Let P be a finite group whose cardinality is a power of p. Let X be a finite set whose cardinality is not divisible by p. Suppose that P is a subgroup of $S(X)$, the group of all pemutations of the set X. Prove: P must fix some point x of X, i.e. $g(x) = x$ for all g in P.

   b. Give an example of a finite set X and a finite subgroup G of $S(X)$ such that the cardinalities of G and X are relatively prime, but G fixes no point of X.

3. Let T be a linear transformation on a finite dimensional vector space V over $\mathbb{R}$ (the real numbers). Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{R}[x]$ with $(f, g) = 1$. Let

$$V_0 = \{v \in V : f(T)(v) = 0\} \quad \text{and} \quad V_1 = \{v \in V : g(T)(v) = 0\}.$$

Prove:

   a. V_0 and V_1 are T-invariant subspaces of V and $V_0 \cap V_1 = \{0\}$.

   b. If $m(x)$ is the minimum polynomial of T on V and if $m(x) = f(x)g(x)$ with f and g as above, then $V = V_0 \oplus V_1$.

4. Let $\mathbb{R}^n$ be Euclidean n-space with the standard inner product denoted by $(\, , \,)$. Let $f : \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation. Let M be the matrix of f relative to the standard orthonormal basis for $\mathbb{R}^n$

Def: f is an *isometry* if $(f(x), f(y)) = (x, y)$ for all $x, y \in \mathbb{R}^n$.

Def: The matrix M is *orthogonal* if $M^t \cdot M = I_n$. (Here M^t is the transpose of M and I_n is the identity matrix.)

Prove: The linear transformation f is an isometry if and only if its matrix M is orthogonal.

5. Let R be a commutative ring with 1. An ideal P of R is *prime* if whenever a and b are in R and ab is in P, then either a is in P or b is in P.

   a. Prove: If M is a maximal ideal of R, then M is prime.

   b. Give an example of a commutative ring R and prime ideal P which is not maximal. Give a proper maximal ideal M containing P.

6. a. Let $p(x)$ be a polynomial of degree 4 which factors as a product of two quadratic polynomials with rational coefficients. List all possibilities for the Galois group of $p(x)$ over $\mathbb{Q}$ (the rational numbers) with examples for each.

   b. Let $p(x) = x^4 - 5x^2 + 6$. Determine the Galois group G of $p(x)$ over $\mathbb{Q}$. List all subgroups of G and the intermediate fields to which they correspond under the Galois correspondence.