Qualifying Exam in Algebra
Spring 2016

Answer each of the following questions clearly and concisely. All answers count.

1. Let G_1 and G_2 be finite groups and p be a prime integer.

   (a) Show that the subgroup $Q \leq G_1 \times G_2$ is a Sylow p-subgroup if and only if $Q = P_1 \times P_2$ for some Sylow p-subgroups $P_1 \leq G_1$ and $P_2 \leq G_2$.

   (b) Determine (with proof) the number of Sylow 2-subgroups of $S_3 \times S_4$, where S_n denotes the symmetric group on n letters.

2. Let G be a group and $G' = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$ be the commutator subgroup of G. (That is, G' is the subgroup of G generated by all of the commutators $xyx^{-1}y^{-1}$).

   (a) Show that, if $H \lhd G$ is a normal subgroup such that the quotient group G/H is Abelian, then $G' \leq H$.

   (b) Show that, if $H \leq G$ is a subgroup such that $G' \leq H$, then $H \lhd G$ is a normal subgroup and the quotient group G/H is Abelian.

3. Let R be a Boolean ring. (That is, R is a ring with unit element such that $r^2 = r$ for all $r \in R$.)

   (a) Show that $-r = r$ for all $r \in R$.

   (b) Show that R is a commutative ring.

   (c) Show that every prime ideal of R must be maximal.

4. Let R be a ring with unit element and $\theta : \mathbb{Z} \to R$ the canonical ring homomorphism such that $\theta(1) = 1$. Suppose that R contains exactly p^2 elements for some prime integer p.

   (a) Show that, if θ is not surjective, then the image of θ is a field containing exactly p elements.

   (b) Show that R is a commutative ring.

5. Let α be a root of the polynomial $f = X^4 + 1$ in the field $\mathbb{C}$ of complex numbers.

   (a) Show that $\mathbb{Q}(\alpha)$ is a splitting field for f over the field $\mathbb{Q}$ of rational numbers.

   (b) Determine the Galois group of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

   (c) Determine all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$, and identify the corresponding subgroups of the Galois group.

6. Suppose that E is a finite extension field of the field F, and $f \in F[X]$ is an irreducible polynomial of prime degree p such that f is reducible in $E[X]$. Show that p divides the degree $[E : F]$.

Qualifying Exam in Algebra
Fall 2015

Answer each of the following questions clearly and concisely. All answers count.

1. Let G be a finite group and $Z(G)$ its center, that is, $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$.

   (a) Show that, if $G/Z(G)$ is cyclic, then G is abelian.

   (b) Show that, if G is a nonabelian p-group for some prime p, then $|G| > p^2$.

2. Let $\sigma = (1, 2, 3, 4, 5)$, a 5-cycle in the symmetric group S_5.

   (a) Determine the centralizer $C_{S_5}(\sigma)$ of σ in S_5, that is, $C_{S_5}(\sigma) = \{\tau \in S_5 \mid \sigma\tau = \tau\sigma\}$.

   (b) Show that there is a 5-cycle in S_5 which is *not* conjugate to σ in the alternating group A_5.

3. Find three pairwise nonisomorphic rings with identity, each of cardinality 25, and show that they are pairwise nonisomorphic.

4. Let R be a commutative ring with identity, and recall that an element $r \in R$ is called *nilpotent* if $r^n = 0$ for some positive integer n.

   (a) Show that the set of all nilpotent elements of R forms an ideal of R.

   (b) Let $f = a_0 + a_1X + \ldots + a_mX^m$ be a polynomial in X with coefficients in R. Show that f is nilpotent in the polynomial ring $R[X]$ if and only if $a_0, a_1, \ldots, a_m$ are all nilpotent in R.

5. Let $f = X^4 - 2$ in $\mathbb{Q}[X]$, and let K be a splitting field of f over $\mathbb{Q}$.

   (a) Determine a generating set for K over $\mathbb{Q}$, and the degree $[K : \mathbb{Q}]$.

   (b) Show that the Galois group of K over $\mathbb{Q}$ is isomorphic to a dihedral group.

6. Let p be a prime and n a positive integer, and let $\mathbb{F}_{p^n}$ denote a finite field of cardinality p^n.

   (a) Show that the function $\psi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by $\psi(a) = a^p$, is a field automorphism of $\mathbb{F}_{p^n}$, and that $\psi(a) = a$ for every $a \in \mathbb{F}_p$.

   (b) Show that ψ^n is the identity automorphism of $\mathbb{F}_{p^n}$, but that, for every positive integer $k < n$, ψ^k is *not* the identity automorphism of $\mathbb{F}_{p^n}$.

Department of Mathematical Sciences
January 16, 2015 Name: ____________________

Qualifying Exam in Algebra$_{\text{vf}}$

There are five problems. All answers count.

PROBLEM 1: (a) What is meant by the *cycle type* of a permutation in S_n?

Show that two permutations in S_n are conjugate if and only if they have the same cycle type.

Prove that the normal subgroups of S_3 are $\{e\}$, A_3, S_3.

(b) Treating the different cases of $n \in \mathbb{N}$ suitably, determine all homomorphisms from S_3 to C_n (the cyclic group of order n).

PROBLEM 2: Let p be a prime and G a group of order p^n. Prove that any nontrivial normal subgroup of G has a nontrivial intersection with the center of G.

PROBLEM 3: (a) Suppose G is a group in which the element g has finite order m. For r an integer, state a formula for the order of g^r and prove it.

(b) Assume now that G is a nontrivial finite abelian p-group. Prove that G is cyclic if and only if G has exactly $p-1$ elements of order p.

PROBLEM 4: (a) Let $f(x) \in F[x]$ be a polynomial with coefficients in a field F. Show that $f(x)$ has a multiple root (in its splitting field) if and only if the polynomial $f(x)$ and its formal derivative $f'(x)$ have a nontrivial common factor.

(b) Let $f(x)$ be an irreducible polynomial $f(x)$ over a field F. Show that $f(x)$ has a multiple root if and only if the characteristic of F is $p > 0$ and $f(x) = g(x^p)$ for some polynomial $g(x)$.

(c) Is it possible for an irreducible polynomial over the field $\mathbb{F}_2$ of 2 elements to have a multiple root? Give an example or show that this is not possible.

PROBLEM 5: Let $f(x) = x^4 - 3$. Find the Galois group of $f(x)$ over each of the following fields.

(a) $\mathbb{Q}$

(b) $\mathbb{Q}(i)$

Department of Mathematical Sciences
August 25, 2014 Name: ____________________

Qualifying Exam in Algebra$_{\text{vb}}$

There are six problems. All answers count.

PROBLEM 1: (a) Let G be a finite group. Show that any two conjugacy classes in G are either equal or disjoint. Prove that any normal subgroup of G is a disjoint union of conjugacy classes.

(b) For $G = S_4$, the symmetric group on 4 letters, find all normal subgroups.

PROBLEM 2: Let G be the symmetric group on p letters where p is a prime number. Prove that if a subgroup H of G contains a p-cycle and a transposition, then $H = G$.

PROBLEM 3: Suppose R is a commutative ring, and I, J are ideals in R with $I \subset J$.

(a) Show that $J' = J/I$ is an ideal in $R' = R/I$.

(b) Show that the rings R/J and R'/J' are isomorphic.

(c) Let $k = \mathbb{F}_2$ be the field of 2 elements.
Deduce that $k[x, y]/(x^2 + x + 1, y^3 + y + 1)$ is a field.

PROBLEM 4: Suppose p is a prime number. If $f(x)$ is an irreducible polynomial of degree p over $\mathbb{Q}$ having exactly two non-real roots, then show that the Galois group of the splitting field of $f(x)$ is the symmetric group S_p on p letters.

Hint: You may use the result of Problem 2.

PROBLEM 5: Let $\zeta = e^{\frac{2\pi i}{8}}$ be a primitive 8-th root of unity and let $K = \mathbb{Q}(\zeta)$. Determine the Galois group $G = \mathrm{Gal}(K, \mathbb{Q})$, and for each subgroup $H \subset G$, determine the fixed field K_H.
Hint: Decide if $i \in K$. Is $\sqrt{2} \in K$?

PROBLEM 6: Let k be a field. A module M over the polynomial ring $k[x]$ is called *nilpotent* if $x^n M = 0$ for some $n \in \mathbb{N}$.

(a) Show that the $k[x]$-module $k[x]/(x^m)$ is a k-vector space of dimension m.

(b) Show that every cyclic nilpotent $k[x]$-module is isomorphic to $k[x]/(x^m)$ for some $m \in \mathbb{N}$.

(c) Find all nilpotent $k[x]$-modules of k-dimension 5, up to isomorphy.

Algebra Qualifier Exam, January 21, 2014.

(1) Let $G = \langle a \rangle$ be a finite cyclic group of order n, written multiplicatively. For a positive integer m, let $\varphi : G \to G$ be the map defined by $\varphi(x) = x^m$.
  (a) Prove that φ is a homomorphism.
  (b) Determine the order of the image of φ.
  (c) Determine the order of the kernel of φ.
  (d) Find necessary and sufficient conditions on m such that φ is an automorphism.

(2) Let G be a group of order p^2q, where p and q are distinct prime numbers. Prove:
  (a) G contains a proper normal subgroup.
  (b) G is solvable.

(3) Let K denote the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ of the field $\mathbb{Q}$ of rational numbers.
  (a) Show that K is normal over $\mathbb{Q}$. In particular, specify a monic polynomial $f \in \mathbb{Q}[x]$ for which K is the splitting field and determine the Galois group.
  (b) Show that the intermediate fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ are isomorphic as $\mathbb{Q}$-vector spaces, but not isomorphic as fields.

(4) Let k be a field and A a k-algebra such that the dimension of A as a k vector space is n. Let α be an element of A. Prove the following.
  (a) There exists a monic polynomial $f \in k[x]$ satisfying
    (i) $f(\alpha) = 0$ and
    (ii) if $g \in k[x]$ and $g(\alpha) = 0$, then $f \mid g$.
  (b) Let f denote the polynomial of part (a). If the degree of f is n, then α generates A as a k-algebra and A is commutative.

(5) Let $f = x^3 - 1$ and $g = x^6 - 2x^3 + 1$ be polynomials in $\mathbb{Q}[x]$, where $\mathbb{Q}$ is the field of rational numbers. Let $R = \mathbb{Q}[x]/(f)$ and $S = \mathbb{Q}[x]/(g)$.
  (a) Show that there is a surjective homomorphism of rings $S \to R$.
  (b) Show that R is isomorphic to a direct product $F_1 \times F_2$ of two fields. You should carefully describe the fields F_1, F_2, and the isomorphism.
  (c) Determine $\operatorname{rad}(R)$ and $\operatorname{rad}(S)$.
  (For any commutative ring A, $\operatorname{rad}(A)$, called the *nil radical of* A, is defined to be $\{a \in A \mid a^n = 0 \text{ for some } n \geq 1\}$.)

(1) Show how to construct two nonisomorphic nonabelian groups of order $4 \cdot 17$ each of which is a semidirect product of two cyclic groups.

(2) Let G be a finite group and p a prime. A theorem of Cauchy says that if p divides the order of G, then G contains an element of order p. Prove this in two parts.
  (a) Prove it when G is abelian.
  (b) Use the class equation to prove it when G is nonabelian.

(3) Let k be a field and A a k-algebra which is finite dimensional as a k-vector space. Let α be an element of A. Prove the following statements.
  (a) There exists a monic polynomial $f \in k[x]$ satisfying
    (i) $f(\alpha) = 0$ and
    (ii) if $g \in k[x]$ and $g(\alpha) = 0$, then $f \mid g$.
  (b) If $f(x)$ denotes the polynomial of part (a), then α is invertible in A if and only if $f(0) \neq 0$.

(4) Let $f = (2x^2 - 4x + 1)(x^4 + 1)$. Find a splitting field and determine the Galois group of f over each of the following fields:
  (a) $\mathbb{Q}$
  (b) $\mathbb{Q}(\sqrt{2})$
  (c) $\mathbb{Q}(i)$
  (d) $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/8}$ is a primitive eighth root of 1 in $\mathbb{C}$
  (e) $\mathbb{R}$

(5) For each of the following, either exhibit an example (with proof) of such a ring, or prove that no such ring exists. By assumption, a ring always contains a unit element.
  (a) A field with 16 elements.
  (b) A commutative ring with 16 elements which is not a field and which has no nonzero nilpotent elements.
  (c) A commutative ring with 16 elements which is not a field and which has no nontrivial idempotents.
  (d) A commutative ring with 16 elements which is not a field and which has no nonzero zero divisor.

Department of Mathematics Sciences, FAU Name: ____________________
Date:

Qualifying Examination in Algebra

Instructions: Do the following six problems. When using a theorem be sure to explicitly state the theorem, then apply. Include definitions of terms when needed.

1. Let $p < q$ be distinct primes. Classify the groups of order pq. [Hint: consider two cases: when $p|q-1$ and otherwise.]

2. (a) State and prove the Class Equation for finite groups.
   (b) Suppose G is a group of order p^n $(n \geq 1)$. Prove that the center of G is non-trivial.

3. Let $n \geq 2$ and $\mathbb{Z}_n$ denote the finite cyclic group of order n. Prove that $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to the group of multiplicative units of $\mathbb{Z}_n$.

4. Let $F \leq K$ be an extension of fields and let $u \in K$. State what it means for u to be algebraic over F and define $[F(u) : F]$. Prove that if $[F(u) : F]$ is odd, then $F(u^2) = F(u)$.

5. State and prove the Chinese Remainder Theorem for commutative rings with identity.

6. (a) Find a splitting field for the polynomial $f(x) = x^4 - 2$ over $\mathbb{Q}$ and its degree.
   (b) Determine the Galois group of f over $\mathbb{Q}$.

Department of Mathematical Sciences, FAU
Date: September 4^{th}, 2012, 2-5pm, SE 215

Name: ______________________________

Qualifying Examination Algebra

Instructions: Do the following six problems. When using a theorem be sure to explicitly state the theorem, then apply.

1. State and prove Lagrange's Theorem.

2. Classify all groups (up to isomorphism) of order 28. [Hint: recognize such a group as a semi-direct product.]

3. (a) State Sylow's First Theorem.
   (b) Prove that if G is a group of order $231 = 3 \cdot 7 \cdot 11$, then there is a unique Sylow 7-subgroup of G.
   (c) Prove that if G is a group of order 231, then there is a unique Sylow 11-subgroup of G which is contained in $Z(G)$.

4. (a) Suppose R is a principal ideal domain. Define an irreducible element of R and prove that $a \in R$ is irreducible if and only if aR is a maximal ideal of R.
   (b) Construct a field of $343 = 7^3$ elements. Make sure to explain the results you are using.

5. Suppose $F \leq K \leq L$ is a tower of fields. Define what the symbol $[K : F]$ means and prove that
$$[L : F] = [L : K][K : F]$$
   You may assume that both $[L : K], [K : F] < \infty$.

6. Let $E = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$. Find the minimal polynomial for $\alpha = \sqrt{2 + \sqrt{2}}$ over $\mathbb{Q}$; explain why the polynomial is minimal. Determine $\mathrm{Gal}(E|\mathbb{Q})$ and construct the lattice of subfields E.

Department of Mathematical Sciences
January 6, 2012 Name: ____________________

Qualifying Exam in Algebra$_{\text{v3}}$

There are six problems. All answers count.

PROBLEM 1: (a) List all groups of order six and of order nine, up to isomorphism. Give brief reasons for your answers.

(b) For each pair (A, B) where A is a group of order six, and B a group of order nine, find the number of group homomorphisms from A to B. Give brief reasons for your answers.

1	2	3	4	5	6	Sum

PROBLEM 2: Find all groups of order $5^2 \cdot 7^2$, up to isomorphism.

PROBLEM 3: For each of the following statements, tell whether the statement is true or false, and justify your answer.

(a) $\mathbb{R}[x, y, z]$ is an integral domain.

(b) $\mathbb{R}[x, y, z]$ is a Euclidean ring.

(c) $\mathbb{R}[x, y, z]$ is a unique factorization domain.

(d) $\mathbb{R}[x, y, z]$ is a principal ideal domain.

PROBLEM 4: (a) Suppose F is a field and $p(x) \in F[x]$. Give the definition of a *splitting field* over F for $p(x)$.

(b) State a result regarding the existence and uniqueness of splitting fields.

(c) Let now K be the splitting field for $p(x) = x^6 - 1$ over the field of rational numbers $\mathbb{Q}$. Determine the degree $[K : \mathbb{Q}]$.

(d) For K as in (c), find all 6-th roots of unity in K.

PROBLEM 5: (a) State the Fundamental Theorem of Galois Theory.

(b) Find the Galois group and illustrate the Galois correspondence in the example of the splitting field of the polynomial

$$x^3 - 7$$

over the rational numbers.

PROBLEM 6: Suppose that m is an integer which is not a perfect square, and a, b are rational numbers.

(a) Show that if $a + b\sqrt{m}$ is a root of a polynomial $p(x)$ in $\mathbb{Q}[x]$, then $a - b\sqrt{m}$ is also a root of $p(x)$.

(b) Is the above statement still true if m is a perfect square?

Department of Mathematical Sciences
August 19, 2011 Name: ______________________

Qualifying Exam in Algebra$_{v3}$

There are six problems. All answers count.

PROBLEM 1: (a) List all groups of order four and of order six, up to isomorphism.

(b) For each pair (A, B) where A is a group of order four, and B a group of order six, find the number of group homomorphisms from A to B.

1	2	3	4	5	6	Sum

Problem 2: Suppose $f : G \to H$ is a homomorphism of groups which is onto and which has kernel K.

(a) Show that f induces a one-to-one correspondence between the subgroups of G which contain K and the subgroups of H.

(b) Show that under this correspondence, normal subgroups correspond to normal subgroups.

(c) Suppose N is a normal subgroup of G containing K and $M = f(N)$. Show that f induces an isomorphism

$$\bar{f} : \quad G/N \;\to\; H/M.$$

PROBLEM 3: Let G be a finite group and P a p-Sylow subgroup. For a subgroup H of G write

$$N(H) = \{g \in G : gHg^{-1} = H\}.$$

(a) Show that P is the only p-Sylow subgroup of $N(P)$.

(b) If an element $g \in N(P)$ satisfies $g^{p^m} = e$ for some m, show that $g \in P$.

(c) Show that $N(N(P)) = N(P)$.

PROBLEM 4: (a) Find an irreducible polynomial of degree 6 over the field $\mathbb{F}_2$ of two elements.

(b) Construct a field of 64 elements.

PROBLEM 5: (a) State the Fundamental Theorem of Galois Theory.

(b) Find the Galois group and illustrate the Galois correspondence in the example of the splitting field of the polynomial

$$x^3 - 5$$

over the rational numbers.

PROBLEM 6: (a) Show that the multiplicative group of any finite field is cyclic.

(*Hint:* You may want to show first that a finite abelian group G is cyclic if for each n the relation $x^n = e$ has at most n solutions.)

(b) Deduce that the equation

$$x^2 \equiv -1 \bmod p$$

has a solution in the integers if and only if the odd prime number p satisfies $p \equiv 1 \bmod 4$.

1. If a is a nonzero element of a field, we let $\operatorname{ord} a$ denote the order of a in the multiplicative group of nonzero elements of that field.

   (a) Let f be an irreducible polynomial over a field F. Show that if a and b are roots of f in extension fields of F, then $\operatorname{ord} a = \operatorname{ord} b$.

   (b) Define the **order** of an irreducible polynomial f over F to be $\operatorname{ord} a$ where a is root of f in some extension field of F. Assuming that the polynomials $x^7 + x + 1$ and $x^9 + x + 1$ are irreducible over the two-element field F, find their orders.

2. Let n be a positive integer and F a field of characteristic 0. Let G the Galois group of $x^n - 1$ over F and $\mathbf{Z}_n^*$ the (multiplicative) group of units of the ring of integers modulo n. Show that G is isomorphic to a subgroup of $\mathbf{Z}_n^*$.

3. A commutative ring R is said to be **local** if, for each $r \in R$, either r or $1 - r$ has a multiplicative inverse.

   (a) Show that the ring $\mathbf{Z}_n$ is local if n is a power of a prime number.

   (b) Show that if R is local, and n is the smallest positive integer such that $n \cdot 1 = 0$ in R, then n is a power of a prime number.

4. Show that any group of order 280 has a normal Sylow subgroup.

5. Find a Sylow 2-subgroup of S_5. How many Sylow 2-subgroups does S_5 have?

6. Show that $\mathbf{Z}\left[i\sqrt{3}\right]$ is not a unique factorization domain. Find an ideal in $\mathbf{Z}\left[i\sqrt{3}\right]$ that is not principal

1. Let F be a field and $F[X]$ the ring of polynomials with coefficients in F.

   (a) Define what it means for a polynomial in $F[X]$ to be *irreducible*.

   (b) Define what it means for two polynomials in $F[X]$ to be *relatively prime*.

   (c) Let K be an arbitrary extension field of F.

      i. Prove or disprove: if a polynomial is irreducible in $F[X]$, then it is irreducible in $K[X]$.

      ii. Prove or disprove: if two polynomials are relatively prime in $F[X]$, then they are relatively prime in $K[X]$.

2. Let K be a field, G a finite group of automorphisms of K, and F the fixed field of G.

   (a) Show that K is a separable algebraic extension of F.

   (b) Show that K is a finite-dimensional extension of F of dimension equal to the order of G.

   (c) Show that K is the splitting field of a separable polynomial with coefficients in F.

3. Show that if A is a finite abelian group of order n, and m is a positive integer dividing n, then A has a subgroup of order m. Show that S_5 does not have a subgroup of order 15.

4. Let p be a prime and G a group of order p^n. Prove that a nontrivial normal subgroup of G has a nontrivial intersection with the center of G.

5. Let R be a commutative ring. Show that the polynomial ring $R[X]$ is a principal ideal domain if and only if R is a field.

6. Let f be the minimal polynomial of a square matrix A with entries in a field. Show that A is invertible if and only if $f(0) \neq 0$.

Graduate Qualifying Examination
Segment I / Algebra
January 6, 2010

Instructions

1. There are 2 parts to this exam, each part containing 5 problems.
2. Answer 6 of the questions. Your selection should contain 3 questions from each part. Note that some questions have several components.
3. Indicate clearly which questions you wish to be marked. If you do not do so, the first 3 solutions which you submit from each part will be graded.
4. All answers and proofs should be clearly written. Presentation is as important as the correctness of your results.
5. You have three hours to complete the exam. Good Luck!

PART I

Question 1

Let H be a normal subgroup of a finite group G, and suppose that a prime divisor p of $|G|$ does not divide $[G : H]$. Show that H contains every Sylow p-subgroup of G.

Question 2

(a) The *exponent* of a group G is the least positive integer n such that for all $x \in G$ x^n is the identity of G. Show that every finite abelian group of exponent n contains an element of order n.

(b) Give an example to show that the conclusion of (a) need not be true for non-abelian groups.

Question 3

Consider the symmetric group $\mathcal{S}_7$, and the alternating group $\mathcal{A}_7$.

(a) Determine the conjugacy classes of elements of order 6 in $\mathcal{S}_7$ as well as in $\mathcal{A}_7$.

(b) Determine the cardinalities of the conjugacy classes you discussed in (a) above.

Question 4

For any positive integer m let $\mathcal{S}_m$ denote the symmetric group on m symbols. Prove that there is no proper subroup H such that $\mathcal{S}_{n-1} \subset H \subset \mathcal{S}_n$.

Question 5

Suppose that G is a simple group of order 660 that can be represented as a transitive permutation group on $\{1, 2, \ldots, 11\}$.

(a) Determine the number of elements of order 11 in G,

(b) Determine the number of conjugacy classes of elements of order 11 in G.

PART II

Question 6

Let A and B be two matrices in $GL_2(\mathbb{C})$, the group of 2×2 non-singular matrices over the complex field. Suppose that the characteristic equations of A and B are $x^2 + x + 1$ and $x^2 + x + 2$ respectively. Let W be a finite product of the matrices A and B.

(a) Give a simple expression for the number of factors of W that are the matrix B.

(b) Show that A and B do not necessarily commute. [Hint: Find examples among the matrices with rational integer entries.]

Question 7

Let $R = \{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z} \text{ and } b \not\equiv 0 \,(\mathrm{mod}\ 13)\}$.

(a) Show that R is a ring.

(b) Show that $13 \cdot R$ is a proper ideal of R.

(c) Show that $13 \cdot R$ is the unique maximal ideal of R.

Question 8

For $a \in \mathbb{R}$, let $\phi_a : \mathbb{Q}[x] \to \mathbb{R}$ denote the function defined by $\phi_a(f) = f(a)$ (that is, evaluation at a).

(a) Show that ϕ_a is a ring homomorphism.

(b) Determine the kernel of $\phi_{\sqrt{2}}$.

(c) Determine the kernel of ϕ_π.

Question 9

Let F be a field and $f \in F[x]$ a non-zero polynomial. Show that $F[x]/(f)$ is a field if and only if f is irreducible.

Question 10

Let $f(x)$ be an irreducible polynomial of degree n over a field F.

(a) Prove that the splitting field of $f(x)$ over a finite field F is an extension field of dimension n over F.

(b) Give an example of a field F and an irreducible polynomial $f(x)$ of degree n over F where the dimension of the splitting field is not n.

Graduate Qualifying Examination
Segment II / Algebra
August 18, 2009

Instructions

1. There are 2 parts to this exam.
2. Answer 6 of the questions. Your selection should contain 3 questions from each part. Note that some questions have several components.
3. Indicate clearly which questions you wish to be marked. If you do not do so, the first 3 solutions which you submit from each part will be graded.
4. All answers and proofs should be clearly written. Presentation is as important as the correctness of your results.
5. You have three hours to complete the exam. Good Luck!

PART I - Groups

Question 1

(a) Suppose that an element a of a group G has order mn, where $\gcd(m,n) = 1$. Prove that $a = bc$, where $b, c \in G$ have orders m and n respectively, and $b\,c = c\,b$.

(b) Let G be a group and $a, b \in G$. Prove that the elements abb, bab, and bba all have the same order.

Question 2

If G is a group of order 231, prove that its 11-Sylow subgroup is in the center of G.

Question 3

Suppose that a finite group G admits an automorphism σ of order 2 such that σ fixes only the identity of G. Prove that G is abelian.

Question 4

(a) Define the *normalizer* $N_G(H)$, where G is a group and H a subgroup of G.

(b) Suppose that H is a proper subgroup of a finite group G. Prove that

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

Question 5

Suppose that P is a p-Sylow subgroup of a finite group G, and that S is a subgroup of G such that $N_G(P) \leq S$. Prove that S is *self-normalizing*, i.e. that $N_G(S) = S$.

PART II - Rings & Fields

Question 6

Show that $\mathbb{Z}[\sqrt{-5}\,]$ is not a unique factorization domain.

Question 7

Let R be a commutative ring, and recall that $a \in R$ is called *nilpotent* if $a^n = 0$ for some natural number n.

(a) Show that if $a, b \in R$ are both nilpotent, then $a + b$ is also nilpotent.

(b) Show that the polynomial $a_0 + a_1 x + \cdots + a_t x^t$ is nilpotent in $R[x]$ if and only if each of $a_0, a_1, \ldots, a_t$ is nilpotent in R.

Question 8

Consider the polynomial $f = x^3 - 2$ in $\mathbb{Q}[x]$.

(a) Determine the splitting field K of f over $\mathbb{Q}$.

(b) Determine the Galois group G of f over $\mathbb{Q}$.

(c) Determine the intermediate fields between $\mathbb{Q}$ and K, and the corresponding subgroups of G.

Question 9

Suppose that K is a field extension of F. Prove that if a, b in K are *algebraic* over F, then $a + b$ is also algebraic over F.

Question 10

Show that if K and L are subfields of a finite field F so that K is isomorphic to L, then $K = L$.

In the following, $\mathbb{Q}$ denotes the field of rational numbers and p always denotes a prime number.

(1) Let α an element of finite order in a group G. If b is an integer, state a formula for the order of α^b and prove that your formula is correct.

(2) If p is odd, prove the following.
  (a) If G is a group of order $(p-1)p^2$, then G has a unique p-Sylow subgroup.
  (b) There are at least four groups of order $(p-1)p^2$ which are pairwise non-isomorphic.

(3) Let R be a ring and M an R-module with submodules A and B. Show that the set
$$D = \{(x+A, x+B) \mid x \in M\}.$$
is a submodule of $M/A \oplus M/B$ and that the quotient $(M/A \oplus M/B)/D$ is isomorphic to $M/(A+B)$.

(4) Consider the polynomial $f = x^4 + p^2$ in $\mathbb{Q}[x]$. Determine the following.
  (a) The splitting field of f over $\mathbb{Q}$. Call this field K.
  (b) The Galois group of f over $\mathbb{Q}$.
  (c) The lattice of intermediate fields of $K/\mathbb{Q}$. Determine which intermediate fields are normal over $\mathbb{Q}$.

(5) Let k be a field, x an indeterminate, and f, g, h monic quadratic polynomials in $k[x]$. Assume f has two distinct roots in k, g has exactly one root in k, and h is irreducible. Prove the following statements.
  (a) There is an isomorphism of rings $k[x]/(f) \cong k \oplus k$.
  (b) There is an isomorphism of rings $k[x]/(g) \cong k[x]/(x^2)$.
  (c) The rings $k[x]/(f)$, $k[x]/(g)$, and $k[x]/(h)$ are pairwise non-isomorphic.

(6) Let k be a field and A a k-algebra such that $\dim_k(A) = 2$. Prove the following.
  (a) A contains a primitive element. That is, there exists an element α in A such that α generates A as a k-algebra.
  (b) A is commutative.

In the following, $\mathbb{Q}$ denotes the field of rational numbers and p always denotes a prime number.

(1) Let G be a finite group. Prove the following statement. If p divides the order of G, then G contains an element of order p.

(2) Let k be a field and A a k-algebra which is finite dimensional as a k-vector space. Let α be an element of A. Prove the following statements.
   (a) The minimum polynomial of α over k exists and is unique up to associates.
   (b) The element α is invertible in A if and only if 0 is not a root of the minimum polynomial.

(3) Let $f = x^4 - 5$. Find the Galois group of f over each of the following fields.
   (a) $\mathbb{Q}$,
   (b) $\mathbb{Q}(\sqrt{5})$,
   (c) $\mathbb{Q}(i)$,
   (d) $\mathbb{Q}(i\sqrt{5})$.

(4) Let $f = (x^4 + x^3 + 1)(x^6 + 18x^3 - 36x + 12)$. Prove that there is an isomorphism of rings $\phi \colon \mathbb{Q}[x]/(f) \to F_1 \oplus F_2$, where F_1 and F_2 are fields. You should explicitly describe the fields F_1, F_2, and the map ϕ.

(5) Say G is a finite abelian p-group. Prove that G is cyclic if and only if G has exactly $p - 1$ elements of order p.

(6) Suppose k is a field and f is a monic polynomial in $k[x]$ of degree n. Prove that there exists an n-by-n matrix M over k such that the minimum polynomial of M is equal to f.

(7) Suppose F/k is an extension of fields, n is a positive integer, and M is an n-by-n matrix over k. Prove that the rank of M when viewed as a matrix over k is equal to the rank of M when viewed as a matrix over F.

Department of Mathematical Sciences
Instructor: Markus Schmidmeier
Intro Abstract Algebra — January 8, 2008 Name: ________

Qualifying Exam$_{v4}$

There are eight problems. All answers count.

1. Let G be a group.
   (a) Define the *commutator subgroup* G' of G.
   (b) Show that G' is the smallest normal subgroup of G such that G/G' is abelian.

1	2	3	4	5	6	7	8	Sum

2. Recall that D_{10} is the dihedral group of 10 elements.
   (a) Determine all 2-Sylow and all 5-Sylow subgroups of D_{10}.
   (b) Use this information to find all group homomorphisms $D_{10} \to D_{10}$ which are *not* automorphisms.

3.(a) Give the definition of a *Euclidean ring.*

(b) Let R be a Euclidean ring with norm* d. Show that $a \in R$ is a unit if and only if $d(a) = d(1)$.

—

* some authors call d the "degree" or "function" or "valuation"

4.(a) Determine all abelian groups, up to isomorphism, of order

$$2^4 \cdot 5.$$

(b) For each of the groups G in (a): Write G as a product of cyclic subgroups in such a way that the number of factors is minimal.

5.(a) Show that the polynomial

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

is irreducible over $\mathbb{F}_2$.

(b) Let $\omega = \bar{x}$ be the class of x in $K = \mathbb{F}_2[x]/(f)$. Show that ω is a primitive 5-th root of unity in K.

(c) Find the other primitive 5-th roots of unity in K.

(d) Show that the primitive 5-th roots of unity form a basis of K over $\mathbb{F}_2$.

6.(a) Let g be a polynomial with coefficients in the field F. Give the definition of a *splitting field* for g over F.

(b) Show that $K = \mathbb{F}_2[\omega]$ in Problem 5 is a splitting field for f over $\mathbb{F}_2$.

(c) Suppose that $\omega_1, \ldots, \omega_s$ are all the primitive 5-th roots of unity in K. Show that any automorphism of K takes ω to some ω_i.

(d) How many automorphisms are there for K? Describe the structure of the Galois group $G(K, \mathbb{F}_2)$.

(e) Use the fundamental theorem of Galois theory to describe the subfields of K that contain $\mathbb{F}_2$.

(f) For each proper subfield in (e), specify a basis over $\mathbb{F}_2$.

7.(a) Give the definition of *similarity* of two $n \times n$-matrices.

(b) Let K be a field of characteristic different from 2. For each of the following two matrices with coefficients in K, specify a similar matrix in Jordan canonical form.

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$$

(c) What happens in (b) if the field K is of characteristic 2?

8. For a prime number p and natural numbers m and n write $q = p^m$ and $r = p^n$. Let K and L be a finite fields of q and r elements, respectively.
   (a) Show that every $a \in K$ is a root of the polynomial $x^q - x$.
   (b) Show that if m divides n then K is a subfield of L. *Hint:* Consider the automorphism of L given by $b \mapsto b^q$.
   (c) Show that if K is a subfield of L then m divides n.
   (d) Conclude that if m divides n then $p^m - 1$ divides $p^n - 1$.

Algebra Qualifying Exam **Fall 2007**

Name: ____

There are eight problems. All answers count.

1. True or false? Give a proof or a counterexample!
   (a) Every group of prime order is abelian.
   (b) Every group of order p^2 where p is a prime is abelian.
   Hint: You may want to use the result that the center of a finite p-group is non-trivial.
   (c) Every group of order p^3 is abelian.

1	2	3	4	5	6	7	8	Sum

2. Let G be a group of order 70.
   (a) How many 5-Sylow and how many 7-Sylow subgroups are there in G?
   (b) Deduce that every 5-Sylow and every 7-Sylow subgroup is normal in G.
   (c) Show that G has a normal subgroup of order 35.
   (d) Find at least 4 pairwise non-isomorphic groups of order 70.

3. Which of the following results is true? In each case, explain!
   (a) $\mathbb{C}[x, y]$ is an integral domain.
   (b) $\mathbb{C}[x, y]$ is a Euclidean domain.
   (c) $\mathbb{C}[x, y]$ is a principal ideal domain.
   (d) $\mathbb{C}[x, y]$ is a UFD.

4.(a) Show how to get all abelian groups, up to isomorphism, of order

$$2^3 \cdot 3^2 \cdot 5.$$

(b) For each of the groups G in (a): Write G as a product of cyclic groups in such a way that the number of factors is minimal.

5. Define the *degree* $[L : F]$ of a field extension L of F. If L is a finite extension of F, and K is a finite extension of L, show that K is a finite extension of F and the following formula holds:

$$[K : F] \;=\; [K : L] \cdot [L : F]$$

6.(a) When is a complex number ω called a *primitive n-th root of unity?* How many primitive 5-th roots of unity are there?

(b) If ω is a primitve 5-th root of unity, show that $\mathbb{Q}[\omega]$ is the splitting field of the polynomial $x^5 - 1$ over $\mathbb{Q}$. (Hence, $\mathbb{Q}[\omega]$ is a normal extension of $\mathbb{Q}$.)

(c) Suppose that $\omega_1, \ldots, \omega_s$ are all the primitive 5-th roots of unity. Show that any automorphism of $\mathbb{Q}[\omega]$ takes ω to some ω_i.

(d) How many automorphisms are there for $\mathbb{Q}[\omega]$? Describe the structure of the Galois group $G(\mathbb{Q}[\omega], \mathbb{Q})$.

(e) Use the fundamental theorem of Galois theory to describe the set of subfields of $\mathbb{Q}[\omega]$ which contain $\mathbb{Q}$.

(f) Deduce that the regular pentagon can be constructed by straight-edge and compass.

7.(a) When are two square matrices A and B of the same size said to be *similar?*

(b) Show that the matrix N is similar to its transpose N^t:

$$N = \begin{pmatrix} 0 & & & & & \\ 1 & 0 & & \cdots & 0 & \\ 0 & 1 & 0 & & \vdots & \\ & \vdots & \ddots & \ddots & & \\ & 0 & \cdots & \ddots & 0 & \\ & & & & 1 & 0 \end{pmatrix} \qquad N^t = \begin{pmatrix} 0 & 1 & 0 & & & \\ & 0 & 1 & \cdots & 0 & \\ & & 0 & \ddots & \vdots & \\ & \vdots & & \ddots & \ddots & \\ & 0 & \cdots & & 0 & 1 \\ & & & & & 0 \end{pmatrix}$$

(c) Deduce that every Jordan block $N + \lambda \cdot 1$ (where 1 is the identity matrix of the same size as N and $\lambda \in \mathbb{C}$) is similar to its transpose.

(d) Deduce that every square matrix with coefficients in the complex numbers is similar to its transpose.

8. Suppose that K is a finite field of q elements.
   (a) Show that $q = p^m$ for some prime number p and some integer m.
   (b) Prove the following statement: Every $a \in K$ is a root of the polynomial $f(x) = x^q - x$.
   (c) Deduce from (b) that K is a splitting field over $\mathbb{F}_p$ for $f(x)$ and conclude that all fields of q elements are isomorphic.

Algebra Qualifying Examination
January 4, 2007

Paper is available at the front of the room. Use one side only. Nothing on the other side will be considered.

1. Let J_7 be the ring of integers modulo 7. Let G be the set of functions from J_7 to J_7 of the form $ax+b$ with $a, b \in J_7$ and $a \neq 0$. For example, $2x+3$ takes $\theta \in J_7$ to $2\theta + 3 \in J_7$. Multiplication in G is composition of functions, so $2x+5$ composed with $3x+1$ is $2(3x+1)+5 = 6x$ or $3(2x+5)+1 = 6x+2$ depending on which way you compose.

   (a) Show that if the functions $ax+b$ and $cx+d$ are equal, then $a = c$ and $b = d$.

   (b) Show that G has an identity element.

   (c) What is the inverse of $2x+3$? Of $ax+b$?

   (d) What is the order of G?

   (e) What is the normalizer of $x+1$? What is the normalizer of $2x$? What is the center of G?

   (f) How many Sylow subgroups of each order does G have? What are they?

2. Euclidean rings (Euclidean domains)

   (a) What is a Euclidean ring?

   (b) The ring of Gaussian integers, $\{a+bi : a, b \text{ integers}\}$, is a Euclidean ring. Illustrate this statement, and its proof, using the elements $5+2i$ and $1-3i$.

   (c) Show that if a and b are elements of a Euclidean ring R, then there exist elements s and t in R so that $sa+tb$ divides both a and b.

3. Let U_n be the multiplicative group of units in the ring J_n. The elements of U_n are the images in J_n of integers that are relatively prime to n. Consider the groups U_{24}, U_{15}, U_{16}, U_{30}. How many elements does each have? What are the invariants of each? Which of them are isomorphic?

4. Let $\mathbf{Q}$ be the field of rational numbers and consider the vector space $V_n = \{f \in \mathbf{Q}[X] : \deg f < n\}$. Let $\varphi : V_n \to \mathbf{Q}$ be defined as $\varphi(f) = f(2)$. Find a basis for the kernel of φ.

Fall 2006

1. Let p be an odd prime and G a group of order p. Show that G has exactly one automorphism of order two.

2. How many groups of order 45 are there up to isomorphism? Justify your answer.

3. Repeat question 2 for groups of order 46.

4. Let R be a commutative ring, r an element of R, and $f(X)$ a monic polynomial with coefficients in R. Show that $f(r) = 0$ if and only if $X - r$ divides $f(X)$ in the polynomial ring $R[X]$.

5. Let R be a (commutative) integral domain (with identity). Let a and b be elements of R.

   (a) What does it mean to say that d is a greatest common divisor of a and b?

   (b) Show that if d and e are both greatest common divisors of a and b, then $d = ue$ for some unit u in R.

6. Let $R = \mathbf{Z}\left[\sqrt{-5}\right] = \left\{m + n\sqrt{-5} : m, n \in \mathbf{Z}\right\}$.

   (a) Show that the elements 2 and $1 + \sqrt{-5}$ have a greatest common divisor in R.

   (b) Show that the elements $2 + 2\sqrt{-5}$ and 6 do not have a greatest common divisor in R.

7. Let F be a field of characteristic 7, and V a vector space over F with basis $e_0, e_1, \ldots, e_{20}$. Let $T : V \to V$ be a linear transformation such that $Te_0 = 0$ and $Te_i = ie_{i-1}$ for $i = 1, \ldots, 20$.

   (a) Find a basis for the kernel of T.

   (b) Find the minimum polynomial of T.

1/05

Algebra Qualifying Exam

1. Let R be a commutative ring. Suppose that $(p) \subseteq (q)$ are principal prime ideals. Prove that if p is not a zero-divisor, then $(p) = (q)$. (A ring element $x \in R$ is called a *zero-divisor* if there exists a non-zero element $r \in R$ such that $x \cdot r = 0$.)
2. Let R be a commutative local ring with (unique) maximal ideal M. Prove that the only idempotents of R are 0 and 1.
3. Let A be a module over the commutative ring R and let B be a submodule of A. Prove that if B and A/B are finitely generated, then A is finitely generated.
4. Let R be a commutative ring with S a non-empty, multiplicatively closed subset of R. Suppose that I is an ideal of R with $I \cap S = \emptyset$.
   a. Prove: There exists an ideal P of R such that $P \supseteq I$ and P is maximal wth respect to the property that $P \cap S = \emptyset$.
   b. Prove: The ideal P is a prime ideal.
5. Let K be a field with X an indeterminate. Suppose that $f(X) \in K[X]$ factors as
$$f(X) = [p_1^{e_1}(X)] \cdot \cdots \cdot [p_n^{e_n}(X)]$$
   Prove that
$$K[X]/(f(X) \approx K[X]/(p_1^{e_1}(X)) \times \cdots \times K[X]/(p_n^{e_n}(X))$$
6. Let $\mathbb{Q}$ be the field of rational numbers, with X and Y indeterminates.
   a. Prove that the rings
$$\mathbb{Q}[X, Y]/(Y^2 - X^2) \text{ and } \mathbb{Q}[X, Y]/(Y^2 - X)$$
   are not isomorphic.
   b. Prove that the polynomial $X^2 + Y^2 - 1$ is irreducible over $\mathbb{Q}[X, Y]$.
   c. Prove that the polynomial $10X^4 - 21X^3 + 9X^2 + 15X - 33$ is irreducible over $\mathbb{Q}[X]$.
7. Let G be a finite multiplicative group with H and K subgroups of G. Prove that if the order of H and the order of K are relatively prime, then $H \cap K = \{e\}$. What additional condition on H and K must be imposed in order that G be the direct product of H and K ?

Fall 2004

Algebra Qualifying Exam

1. An additive abelian group A is called *divisible* if for each element $a \in A$, and each nonzero integer k, there exists an element $x \in A$ such that $kx = a$.

    1. Prove that the additive group of rational numbers, $\mathbb{Q}$ is divisible.
    2. Prove that no finite abelian group is divisible.

2. Prove that if A is an abelian group of order pq, where p and $q$are distinct prime integers, then A is cyclic. (Hint:You may use Cauchy's Theorem.)

3. Let R be a commutative ring with identity. An element $a \in R$ is called *nilpotent* if there exists a positive integer n such that $a^n = 0$.

    1. Prove: The set N of all nilpotent elements of R is an ideal of R.
    2. Prove: If P is a prime ideal of R, then $P \supseteq N$. Conclude that if $n \in N$, then $1 + n \notin P$.

4. Let R be a commutative ring with identity. Let P be a prime ideal of R and M be a maximal ideal of R. Denote by $R[X]$ the ring of polynomials in one indeterminate over R.

    1. Prove: The set $P[X] = \{f \in R[X] : \text{each coefficient of } f \text{ belongs to } P\}$ is a prime ideal of $R[X]$.
    2. Prove: The set $M[X] = \{f \in R[X] : \text{each coefficient of } f \text{ belongs to } M\}$ is a maximal ideal of $R[X]$.

5. Show that the polynomial $p(X) = X^3 + 9X + 6$ is irreducible in $\mathbb{Q}[X]$. If θ is a root of $p(X)$, find the inverse of θ in $\mathbb{Q}(\theta)$.

6. Let F be a field with α an element of an extension field of F such that α is algebraic over F. If $[F(\alpha) : F]$ is odd, then prove that $F(\alpha) = F(\alpha^2)$.

7. Let K/F be an algebraic extension of fields and let R be a *ring* contained in K and containing F. Show that R is a subfield of K.