Algebra **Ph.D. Entrance Exam** **Fall 2009**

September 3, 2009

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let H, K, N be subgroups of a group G such that H is a subgroup of K. Show that the following are equivalent.
  (a) $H = K$.
  (b) $H \cap N = K \cap N$ and $HN = KN$.

(2) Let G be a semigroup for which the cancellation laws are satisfied.
  (a) Prove that if G is finite, then G is a group.
  (b) Give an example of an infinite semigroup G for which the cancellation laws are satisfied that is not a group.

(3) Let G be a finite group and let P be a Sylow p-subgroup of G. Show that the following conditions are equivalent:
  (a) P is the only Sylow p-subgroup of G;
  (b) P is normal in G.

(4) Let G be a group, let $a \in G$ have order k, and let p be a prime divisor of k. Prove that if $x \in G$ and $x^p = a$, then x has order pk.

(5) Let H be a subgroup of the symmetric group S_n. Prove that the alternating group A_{n+2} has a subgroup isomorphic to H.

(6) Let R be a commutative ring with identity and prime characteristic p and let n be a positive integer. Show that the map $R \to R$ given by $r \mapsto r^{p^n}$ is a homomorphism of rings.

(7) Consider $R = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ as a subring of the reals. R can be considered either as a $\mathbb{Z}$-module or as an R-module. The map $f : R \to R$ is given by $f(a + b\sqrt{2}) = a + b$. Prove or disprove each of the following:
  (a) f is a $\mathbb{Z}$-homomorphism.
  (b) f is an R-homomorphism.

(8) Let $\mathbb{Z}[x]$ be the ring of polynomials with integral coefficients. Show that the ideal $I = (2, x)$ of $\mathbb{Z}[x]$ generated by the set $\{2, x\}$ is not principal.

(9) Let R be a ring, A, B be R-modules, and $f : A \to B$ and $g : B \to A$ be R-module homomorphisms such that $g \circ f$ is the identity map on A. Prove that B is isomorphic to the direct sum of $\operatorname{Im} f$ and $\ker g$.

(10) Let R be a commutative ring and I be an ideal in R. Prove that I is a free R-module if and only if I is a principal ideal in R generated by an element $a \in R$ that is not a zero divisor.

(11) Prove that $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

(12) Let F be an extension field of a field K, and let $u \in F$ be algebraic over K of degree relatively prime to 6. Prove that $K(u) = K(u^3)$.

(13) Let F be an algebraic extension field of a field K and let R be a subring of F such that $K \subseteq R$. Prove that R is a field. Show by giving a counterexample that it necessary to assume that the extension F/K is algebraic.

(14) Let $\alpha \in \mathbb{C}$ be a root of the polynomial $x^3 + 5x + 5$. Find $a, b, c \in \mathbb{Q}$ so that

$$\alpha^{-1} = a\alpha^2 + b\alpha + c.$$

(15) Prove that every algebraically closed field is infinite.

Algebra **Ph.D. Entrance Exam** **Fall 2008**

August 26, 2008

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let G be a group with subgroups K and H where H is abelian, $H \lhd G$ and $K \subseteq H$. Does it follow that $K \lhd G$? What is the answer to the previous question is we assume that H is cyclic? Give a proof or a counterexample for each question.

(2) Show that if N is a normal subgroup of G with $[G : N]$ finite, and if H is a finite subgroup of G such that $[G : N]$ and $|H|$ are relatively prime, then H is a subset of N.

(3) Prove that the symmetric group S_4 is isomorphic to a subgroup of the alternating group A_6.

(4) Let G be a group and H be a subgroup of G of finite index. Prove that there is a normal subgroup N of G of finite index and with $N \leq H$.

(5) Prove that there are no simple group of order 380.

(6) Let R be an integral domain and I, J be nonzero ideals in R. Prove that $I \cap J \neq \{0\}$.

(7) Let $R = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$. Using standard addition and multiplication, R can be considered either as a $\mathbb{Z}$-module or as an R-module. Let $f : R \to R$ be given by $f(a+b\sqrt{2}) = a+b$. Prove or disprove each of the following:

  (a) f is a $\mathbb{Z}$-module homomorphism.

  (b) f is an R-module homomorphism.

(8) Let R be a commutative ring with identity and prime characteristic p and let n be a positive integer. Show that the map $R \to R$ given by $r \mapsto r^{p^n}$ is a homomorphism of rings.

(9) Let R be a ring, A, B be R-modules, and $f : A \to B$ and $g : B \to A$ be R-module homomorphisms such that $g \circ f$ is the identity map on A. Prove that B is isomorphic to the direct sum of $\operatorname{Im} f$ and $\ker g$.

(10) Let R be a commutative ring with identity and I, J be ideals in R. Prove that if $I + J = R$, then $IJ = I \cap J$.

(11) Let E be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Draw the lattice of all of the intermediate fields between $\mathbb{Q}$ and E and find $\operatorname{Gal}(E/F)$ for each of these intermediate fields F.

(12) Let $\mathbb{Q}[x]$ be the ring of polynomials with rational coefficients, $f = x^3 - 2x^2 + 4x + 2 \in \mathbb{Q}[x]$, and let $u \in \mathbb{R}$ be a real root of f. Express $\left(u^2 + 1\right)(u + 2)$ as a linear combination of $1, u, u^2$ with rational coefficients.

(13) Let F be a field extension of $\mathbb{Q}$ with $[F : \mathbb{Q}] = 24$. Prove that the polynomial $x^5 + 2x^4 - 16x^3 + 6x - 10$ has no roots in F.

(14) Let F be a field and K be a splitting field of some polynomial $f(x) \in F[x]$ over F. Let E be the set consisting of all $a \in K$ such that a is the only root in K of the minimal polynomial of a over F. Prove that E is a field.

(15) Let p be a prime. Describe the integers n such that there is a field K of order n and an element $a \in K^\times$ whose order in $K^\times$ is p. (If R is a ring, then $R^\times$ denotes the set of all units in R).

Algebra **Ph.D. Entrance Exam** **Fall 2007**

August 28, 2007

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let $G = \langle a \rangle$ be a cyclic group of order n. Prove that a^k generates G if and only if n and k are relatively prime.

(2) Prove that the union of a nonempty chain of normal subgroups of a group G is a normal subgroup of G.

(3) Let $\varphi : G \to G'$ be a homomorphism of groups with kernel K. Prove that $\varphi^{-1}(\varphi(H)) = HK$ for every subgroup H of G.

(4) Let G be a finite group, H be a subgroup of G, and N be a normal subgroup of G such that $|N|$ and $[G : N]$ are relatively prime. Prove that H is a subgroup of N if and only if $|H|$ divides $|N|$.

(5) Give an example of a group G with normal subgroups A, B, and C such that any two of them have trivial intersection and G is generated by $A \cup B \cup C$, but $G \neq A \oplus B \oplus C$.

(6) Let D be a principal ideal domain and $a, b, c \in D$ with a and b being relatively prime. Prove that if a divides bc, then a divides c.

(7) State and prove the Eisenstein's Criterion.

(8) Let R be a principal ideal domain and $a \in R$ be not a zero and not a unit. Prove that the ideal Ra in R is prime if and only if a is irreducible.

(9) Prove that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

(10) Prove that any finitely generated R-module over a commutative ring R is a homomorphic image of a free R-module.

(11) Let K be a field extension of a field F and $S \subseteq K$ with each $s \in S$ being algebraic over F. Prove that $E = F(S)$ (the field generated by S over F) is algebraic over F.

(12) Let $f(x) = x^3 + x^2 + 1$ and $k(x) = x^3 + x + 1$ be polynomials in $\mathbb{Z}_2[x]$. Let F and K be extensions of $\mathbb{Z}_2$ obtained by adjoining roots of $f(x)$ and $k(x)$ respectively. Describe explicitely an isomorphism from F to K.

(13) Let F be a field and a be an element of some extension of F with $[F(a) : F] = n$. Prove that $1, a, a^2, \ldots, a^{n-1}$ is a basis of $F(a)$ over F.

(14) Let K be a field extension of F generated by $a, b \in K$ of relatively prime degrees m and n over F. Prove that $[K : F] = mn$.

(15) Prove that if F is a finite field, then $|F|$ is a power of a prime.

August 29, 2006

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let H be a subgroup of a group G such that $x^2 \in H$ for every $x \in G$. Prove that $H \lhd G$ and that G/H is abelian.

(2) Let $f : G \to H$ be a group homomorphism, $x \in G$, m be the order of x in G, and n be the order of $f(x)$ in H. Prove that if m is finite, then n is also finite and m is equal to n multiplied by the order of $\langle x \rangle \cap \ker f$.

(3) Let G be a group and let $x \in G$ be an element of order m. Prove that if n is a positive integer such that m and n are relatively prime, then $x = y^n$ for some $y \in G$.

(4) Let $f_1 : G_1 \to H_1$ and $f_2 : G_2 \to H_2$ be group homomorphisms. Prove that $N = \ker f_1 \times \ker f_2$ is a normal subgroup of $G = G_1 \times G_2$ and that G/N is isomorphic to $\operatorname{im} f_1 \times \operatorname{im} f_2$.

(5) Prove that there are no simple group of order 380.

(6) Let R and S be rings with multiplicative identity, and let $f : R \to S$ satisfy $f(ab) = f(a)f(b)$ and $f(a+b) = f(a)+f(b)$ for every $a, b \in R$. Show, by giving an example, that it is possible that $f(1) \neq 1$. Prove that if f is surjective, then $f(1) = 1$.

(7) Let $\mathbb{Q}$ be the ring of rationals and R be an arbitrary ring with multiplicative identity. Prove that if $f, g : \mathbb{Q} \to R$ are ring homomorphisms satisfying $f(1) = g(1) = 1$, then $f = g$.

(8) Let R be a commutative ring with multiplicative identity and let I be an ideal in R. Let J consist of those elements a in R for which there is a nonnegative integer n with $a^n \in I$. Prove that J is an ideal in R.

(9) Let R be a commutative ring with multiplicative identity and I, J be maximal ideals in R. Prove that if $f : R/I \to R/J$ is a nonzero homomorphism of R-modules, then f is surjective.

(10) Let R be a ring with multiplicative identity, M, N be left R-modules, and $f : M \to N$ and $g : N \to M$ be R-module homomorphisms such that $g \circ f$ is the identity map on M. Prove that $N = \operatorname{im} f + \ker g$ and $\operatorname{im} f \cap \ker g = \{0\}$.

(11) Give an example of a commutative ring R with multiplicative identity such that R is not a field, but R has a subring F that is a field and the additive group of R is a finitely dimensional vector space over F, where the scalar multiplication is the multiplication in R.

(12) Let K be a field and $f, g \in K[x]$ be nonzero polynomials over K. Prove that f and g have a nonconstant common factor in $K[x]$ if and only if there is a field extension F of K such that f and g have a common root in F.

(13) Let F be a field, n be a positive integer, and R be the ring of $n \times n$ matrices with entries in F. Prove that for every field extension K of F with $[K : F] \leq n$, there is a subring of R isomorphic to F.

Hint: If K is an extension of F and $a \in K$, then multiplication by a is a linear map $K \to K$ with K considered as a vector space over F.

(14) Let K be a field extension of a field F. Let V be a subspace of the vector space K over F such that $v^n \in V$ for every $v \in V$ and $n \geq 2$. Prove that if $v \in V \setminus \{0\}$ is algebraic over F, then $v^{-1} \in V$.

(15) Prove that every algebraically closed field is infinite.

Algebra **Ph.D. Entrance Exam** **Fall 2006**

August 29, 2006

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let H be a subgroup of a group G such that $x^2 \in H$ for every $x \in G$. Prove that $H \lhd G$ and that G/H is abelian.

(2) Let $f : G \to H$ be a group homomorphism, $x \in G$, m be the order of x in G, and n be the order of $f(x)$ in H. Prove that if m is finite, then n is also finite and m is equal to n multiplied by the order of $\langle x \rangle \cap \ker f$.

(3) Let G be a group and let $x \in G$ be an element of order m. Prove that if n is a positive integer such that m and n are relatively prime, then $x = y^n$ for some $y \in G$.

(4) Let $f_1 : G_1 \to H_1$ and $f_2 : G_2 \to H_2$ be group homomorphisms. Prove that $N = \ker f_1 \times \ker f_2$ is a normal subgroup of $G = G_1 \times G_2$ and that G/N is isomorphic to $\operatorname{im} f_1 \times \operatorname{im} f_2$.

(5) Prove that there are no simple group of order 380.

(6) Let R and S be rings with multiplicative identity, and let $f : R \to S$ satisfy $f(ab) = f(a)f(b)$ and $f(a+b) = f(a)+f(b)$ for every $a, b \in R$. Show, by giving an example, that it is possible that $f(1) \neq 1$. Prove that if f is surjective, then $f(1) = 1$.

(7) Let $\mathbb{Q}$ be the ring of rationals and R be an arbitrary ring with multiplicative identity. Prove that if $f, g : \mathbb{Q} \to R$ are ring homomorphisms satisfying $f(1) = g(1) = 1$, then $f = g$.

(8) Let R be a commutative ring with multiplicative identity and let I be an ideal in R. Let J consist of those elements a in R for which there is a nonnegative integer n with $a^n \in I$. Prove that J is an ideal in R.

(9) Let R be a commutative ring with multiplicative identity and I, J be maximal ideals in R. Prove that if $f : R/I \to R/J$ is a nonzero homomorphism of R-modules, then f is surjective.

(10) Let R be a ring with multiplicative identity, M, N be left R-modules, and $f : M \to N$ and $g : N \to M$ be R-module homomorphisms such that $g \circ f$ is the identity map on M. Prove that $N = \operatorname{im} f + \ker g$ and $\operatorname{im} f \cap \ker g = \{0\}$.

(11) Give an example of a commutative ring R with multiplicative identity such that R is not a field, but R has a subring F that is a field and the additive group of R is a finitely dimensional vector space over F, where the scalar multiplication is the multiplication in R.

(12) Let K be a field and $f, g \in K[x]$ be nonzero polynomials over K. Prove that f and g have a nonconstant common factor in $K[x]$ if and only if there is a field extension F of K such that f and g have a common root in F.

(13) Let F be a field, n be a positive integer, and R be the ring of $n \times n$ matrices with entries in F. Prove that for every field extension K of F with $[K : F] \leq n$, there is a subring of R isomorphic to F.

Hint: If K is an extension of F and $a \in K$, then multiplication by a is a linear map $K \to K$ with K considered as a vector space over F.

(14) Let K be a field extension of a field F. Let V be a subspace of the vector space K over F such that $v^n \in V$ for every $v \in V$ and $n \geq 2$. Prove that if $v \in V \setminus \{0\}$ is algebraic over F, then $v^{-1} \in V$.

(15) Prove that every algebraically closed field is infinite.

Algebra **Ph.D. Entrance Exam** **Fall 2005**

August 29, 2005

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let G be a group with subgroups K and H where H is abelian, $H \lhd G$ and $K \subseteq H$. Does it follow that $K \lhd G$? What is the answer to the previous question is we assume that H is cyclic? Give a proof or a counterexample for each question.

(2) Prove that a group of order 30 has a normal subgroup of order 3 or 5.

(3) Let G be a finite group, $K \lhd G$, and H be a subgroup of G that is not normal with $|K| = |H|$. Prove that $\gcd(|K|, [G : H]) \geq 2$.

(4) Let H be a subgroup of the symmetric group S_n. Prove that the alternating group A_{n+2} has a subgroup isomorphic to H.

(5) Let G be a group with subgroup H such that $[G : H]$ is finite, and $g \in G$. Is it true that the index of gHg^{-1} in G is also finite. Give a proof or a counterexample.

(6) Let K be an extension field of a field F, and let $u \in K$ be algebraic over F of prime degree p. Prove that if m is a positive integer such that $u^m \notin F$, then $F(u) = F(u^m)$.

(7) Let K be an extension field of a field F, and let $u, v \in K$. Prove that if v is algebraic over $F(u)$ and it is transcendental over F, then u is algebraic over $F(v)$.

(8) Let K be an algebraic field extension of a field F. Consider K as a vector space over F, and let V be a subspace of that vector space such that $v^n \in V$ for every $v \in V \setminus \{0\}$ and $n \geq 0$. Prove that if $v \in V \setminus \{0\}$, then $v^{-1} \in V$.

(9) Let $\alpha \in \mathbb{C}$ be a root of the polynomial $x^3 + 4x - 2$. Find $a, b, c \in \mathbb{Q}$ so that

$$(2\alpha + 1)^{-1} = a\alpha^2 + b\alpha + c.$$

(10) Let $\alpha \in \mathbb{C}$ be a root of the polynomial $3x^3 - 5x^2 + 15x - 10$ and $\beta \in \mathbb{C}$ be a root of $x^5 + 2x^4 + 26$. Find $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$.

(11) Let A be an R-module and $f : A \to A$ be an R-module homomorphism such that $f \circ f = f$. Prove that $A = \ker f \oplus \operatorname{Im} f$.

(12) Let R be a commutative ring with identity and I, J be ideals in R. Prove that if $I + J = R$, then $IJ = I \cap J$. Give an example of a ring R and ideals I, J of R such that $IJ \neq I \cap J$.

(13) Let R be a commutative ring and I be an ideal in R. Prove that I is a free R-module if and only if I is a principal ideal in R generated by an element $a \in R$ that is not a zero divisor.

(14) Let R be a commutative ring and M be a finitely generated R-module. Prove that there exists a free R-module N and a surjective R-module homomorphism $f : N \to M$.

(15) Let R be a finite integral domain. Prove that R is a field.

Ph.D. Entrance Examination in Algebra

April 2005
Instructions: Throughout this exam, $\mathbf{R}, \mathbf{Q}, \mathbf{Z}, \mathbf{Z}_m$ represent the real number field, the rational number field, the ring of integers, and the cyclic group of order m, respectively. Work any ten problems. If you turn in partial solutions to more than 10 problems, indicate clearly which 10 should be graded. (Otherwise only the worst 10 problems will be counted.)

1. Let M and N be normal subgroups of G. Show that MN is also a normal subgroup of G.

2. Let G be a finite (multiplicative) abelian group with identity 1. Show that if for any positive integer n, the equation $x^n = 1$ has at most n solutions in G, then G is cyclic.

3. Show that any group of order 65 must be cyclic.

4. Is there a simple group with order 48? (Give your example for the YES answer, and present your proof for the NO answer).

5. Suppose that R is a system that satisfies all the axioms of a ring with a multiplicative identity 1 except the axiom that $a + b = b + a$. Show that in this case, we must have $a + b = b + a$, $\forall a, b \in R$.

6. Suppose that G is a finite group and that p is smallest prime dividing $|G|$. If G has a subgroup H such that $[G : H] = p$, show that there exists an onto homomorphism $\phi : G \mapsto \mathbf{Z}_p$.

7. Let U be an ideal of a ring R. Show that

$$R(U) = \{r \in R \ : \ \forall u \in U, ru = 0\}$$

is an ideal of R.

8. Let $F = \mathbf{Z}_{11}$ denote the field of 11 elements. Are the two quotient rings $F[x]/(x^2 + 1)$ and $F[x]/(x^2 + 6)$ isomorphic? (You must prove or justify your answer.)

9. Let F be a field, and let $n > 1$ be an integer. Show that

$$W = \{a_0 + a_1x + a_2x^2 + \cdots a_{n-1}x^{n-1} \in F[x] \ : \ a_0 + a_1 + \cdots + a_{n-1} = 0\},$$

is a vector space. Find a basis of W over F.

10. Let $E = \mathbf{Q}(\sqrt{5}, \sqrt{7})$. Show that E is a simple extension of $\mathbf{Q}$, and find a polynomial $f(x) \in \mathbf{Q}[x]$ such that $E \cong \mathbf{Q}[x]/(f(x))$.

11. Let $\mathbf{R}$ be a commutative ring, and let M and N be two R-modules. Let $f : M \mapsto N$ be an R-module homomorphism. Show that $K = \{x \in M \ : \ f(x) = 0\}$ is a submodule of M and $W = \{f(x) \in N \ : \ x \in M\}$ is a submodule of N.

12. Let R be a PID, and let $\{a_1, a_2, ..., a_n, ...\}$ be an infinite sequence of elements in R such that for each $n \geq 1$, $a_{n+1}|a_n$ (that is, $a_n = a_{n+1}r_n$ for some $r_n \in R$). Show that there exists an $N > 0$ such that a_m and a_N are associates for every $m \geq N$.

13. Let R be an integral domain and let P be an ideal of R such that R/P is also an integral domain. Show that for any $x, y \in R - P$, $xy \in R - P$. (That is, the multiplication of R, when restricted to the subset $R - P$, is a binary operation.)

14. Let F be a field, $a_1, a_2, \cdots, a_n \in F$ be n distinct elements in F, and for each $i = 1, 2, \cdots, n$, define

$$p_i(x) = \prod_{j=1, j\neq i}^{n} (x - a_i).$$

For any elements $b_1, b_2, \cdots, b_n \in F$, show that the polynomial

$$f(x) = \prod_{i=1}^{n} b_i(p_i(a_i))^{-1}p_i(x),$$

is the unique polynomial in $F[x]$ such that $f(a_i) = b_i$, $i = 1, 2, \cdots, n$.

15. Suppose that $p > 3$ is a prime and that $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is a polynomial in $\mathbf{Q}[x]$. Show that $f(x)$ is irreducible in $\mathbf{Q}[x]$.

Algebra **Ph.D. Entrance Exam** **Fall 2004**

09/02/2004

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

1. Let G be a finite group, p be the smallest prime dividing $|G|$ and H be a subgroup of G of index p. Prove that H is normal in G.
2. Let G be a group, and H be a normal subgroup of G such that H is abelian. Prove that there is a group homomorphism
$$\varphi : G/H \to \mathrm{Aut}\,(H)\,,$$
defined by
$$\varphi(gH) = \sigma_g \quad \text{with } \sigma_g(a) = gag^{-1}$$
where $\mathrm{Aut}(H)$ is the group of isomorphisms $H \to H$ under composition.
3. Let G be a group and H be a subgroup of G of finite index. Prove that there is a normal subgroup N of G of finite index and with $N \leq H$.
4. Let G be a group and H be a subgroup of G of finite index. Prove that G is the union of the conjugates of H if and only if $H = G$.
5. Let K be a normal subgroup of a finite group G, and P be a Sylow p-subgroup of K for some prime p. Prove that
$$KN_G(P) = \{kn : k \in K,\ n \in N_G(P)\}$$
is equal to G, where $N_G(P)$ is the normalizer of P in G.
6. Let R be a commutative ring with identity and a be a nilpotent element of R ($a^n = 0$ for some positive integer n). Prove that $1 + a$ is a unit in R.
7. Prove that the ideal (x, y) generated by x and y in the ring of polynomials of two variables $\mathbb{Q}[x, y]$ is not principal.
8. Let R be a commutative ring with identity and I, J be ideals in R. Prove that if $I + J = R$, then $IJ = I \cap J$.
9. Let R be a commutative ring and I be an ideal in R. Prove that I is a free R-module if and only if I is a principal ideal in R generated by an element $a \in R$ that is not a zero divisor.
10. Determine the number of isomorphism classes of abelian groups of order 400.
11. Let α be a root of the polynomial $x^3 + 3x + 1$. Prove that α can not be constructed by ruler and compass.
12. Let K/F be a field extension and $a \in K$ be algebraic over F. Prove that $a + 1$ is algebraic over F.

13. Let K be a field extension of $\mathbb{Q}$ with $x^3 + 5x^2 - 15x + 10$ and $x^5 + 3x^2 - 30x + 6$ having roots in K. Prove that $[K : \mathbb{Q}] > 11$.
14. Let $\alpha \in \mathbb{C}$ be a root of the polynomial $x^3 + 3x + 3$. Find $a, b, c \in \mathbb{Q}$ so that
$$\alpha^{-1} = a\alpha^2 + b\alpha + c.$$
15. Let F be a field and K be a splitting field of some polynomial $f(x) \in F[x]$ over F. Let E be the set consisting of all $a \in K$ such that a is the only root in K of the minimal polynomial of a over F. Prove that E is a field.

Algebra **Ph.D. Entrance Exam** **Fall 2003**

8/27/03

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let G be a group, let $a \in G$ have order k, and let p be a prime divisor of k. Prove that if $x \in G$ and $x^p = a$, then x has order pk.

(2) Prove that the intersection of any family of normal subgroups of a group G is itself a normal subgroup of G.

(3) Let G be a finite group and K be a normal subgroup of G. Prove that if $|K|$ and $[G : K]$ are relatively prime, then K is the unique subgroup of G of order $|K|$.

(4) Let G be a subgroup of S_n with more that 2 elements. Prove that if G is simple, then G is a subgroup of A_n.

(5) Let K be a field and $K(x)$ be the field of rational functions with coefficients in K. Prove that if $f \in K(x)$, then $f^2 \neq x^2 - 1$.

(6) Let R be an integral domain and I, J be nonzero ideals in R. Prove that $I \cap J \neq \{0\}$.

(7) Let K be a field and I be the ideal in the polynomial ring $K[x, y]$ generated by the set $\{x, y\}$. Prove that I is not a principal ideal.

(8) Let $F \subseteq K \subseteq L$ be a tower of fields and $a \in L$. Prove that if $[F(a) : F]$ is finite, then $[K(a) : K]$ is also finite.

(9) Let $\mathbb{F}_8$ be a finite field with 8 elements. Prove that $\mathbb{F}_8$ has no subfield with 4 elements.

(10) Let α be a complex root of the irreducible polynomial $x^3 - 3x + 4$. Find the multiplicative inverse of $\alpha^2 + \alpha + 1$ in $\mathbb{Q}[\alpha]$ explicitely in the form $a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Q}$.

(11) Let α be a complex root of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ and β be a complex root of an irreducible polynomial $g(x) \in \mathbb{Q}[x]$. Prove that $f(x)$ is irreducible in $K[x]$ (where $K = \mathbb{Q}[\beta]$) if and only if $g(x)$ is irreducible in $F[x]$ (where $F = \mathbb{Q}[\alpha]$).

(12) Let K be a field and F be an algebraic field extension of K. Prove that if R is a ring such that $K \subseteq R \subseteq F$, then R is a field.

(13) Let F be a field extension of $\mathbb{Q}$ with $[F : \mathbb{Q}] = 24$. Prove that the polynomial $x^5 + 2x^4 - 16x^3 + 6x - 10$ has no roots in F.

(14) Let R be a ring, A, B be R-modules, and $f : A \to B$ and $g : B \to A$ be R-module homomorphisms such that $g \circ f$ is the identity map on A. Prove that B is isomorphic to the direct sum of $\operatorname{Im} f$ and $\ker g$.

(15) Prove that no nontrivial finite abelian group can be given a structure of a $\mathbb{Q}$-module.

Algebra **Ph.D. Entrance Exam** **Spring 2002**

4/25/02

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let H be a subgroup of a group G with index $[G : H] = 2$.
  (a) Show that H is normal in G.
  (b) Show that $x^2 \in H$ for every $x \in G$.

(2) Let G be a finite group and let P be a Sylow p-subgroup of G. Show that the following conditions are equivalent:
  (a) P is the only Sylow p-subgroup of G;
  (b) P is normal in G.

(3) Let G be a group that has only finitely many subgroups. Prove that G is finite.

(4) Let G be a group and H, K be subgroups of G.
  (a) Prove that if G is isomorphic to the direct product $H \times K$, then H is isomorphic to the quotient group G/K.
  (b) Show that the above implication cannot be reversed, that is, give an example of a group G and subgroups H, K of G such that H is isomorphic to G/K but G is not isomorphic to $H \times K$.

(5) Prove that the symmetric group S_4 is isomorphic to a subgroup of the alternating group A_6.

(6) Show that if N is a normal subgroup of G with $[G : N]$ finite, and if H is a finite subgroup of G such that $[G : N]$ and $|H|$ are relatively prime, then H is a subset of N.

(7) Let R be a finite commutative ring with at least one non-zero divisor. Show that R has a multiplicative identity.

(8) Let D be an integral domain. Prove that if D is finite, then it is a field.

(9) Let $\mathbb{Z}[x]$ be the ring of polynomials with integral coefficients. Show that the ideal $I = (2, x)$ of $\mathbb{Z}[x]$ generated by the set $\{2, x\}$ is not principal.

(10) Let R be a ring, A, B be R-modules, and $f : A \to B$ and $g : B \to A$ be R-module homomorphisms such that $g \circ f$ is the identity map on A. Prove that B is isomorphic to the direct sum of $\operatorname{Im} f$ and $\ker g$.

(11) Let F be an algebraic extension field of a field K and R be a ring such that $K \subseteq R \subseteq F$. Prove that R is a field.

(12) Let $K \subseteq F$ be fields and let $u, v \in F$ be algebraic over K. Prove that $u^2 - v \in F$ is also algebraic over K.

(13) Let $\mathbb{Q}[x]$ be the ring of polynomials with rational coefficients, $f = x^3 - 2x^2 + 4x + 2 \in \mathbb{Q}[x]$, and let $u \in \mathbb{R}$ be a real root of f. Express $(u^2+1)(u+2)$ as a linear combination of $1, u, u^2$ with rational coeficients.

(14) Let $\mathbb{Q}, \mathbb{R}$ be the fields of rational and real numbers respectively.

(a) Prove that $\mathbb{Q}(\sqrt[3]{7}) \subseteq \mathbb{R}$ is not a Galois extension of $\mathbb{Q}$.

(b) Prove that $\mathbb{Q}(\sqrt{7}) \subseteq \mathbb{R}$ is a Galois extension of $\mathbb{Q}$.

(15) Let $F \subseteq K$ be fields with K being algebraic over F and such that for every field extension E of K and any $\sigma \in \operatorname{Aut}_F E$, the restriction of σ to K belongs to $\operatorname{Aut} K$. Show that K is normal over F.

Ph.D. Entrance Examination in Algebra

August 2001

Directions: Work any ten problems. If you turn in partial solutions to more than 10 problems, indicate clearly which 10 should be graded.

1. Let G be a semigroup for which the cancellation laws are satisfied.

   (a) Prove that if G is finite, then G is a group.

   (b) Give an example of an infinite semigroup G for which the cancellation laws are satisfied that is not a group.

2. Prove that if G is an abelian group, then the join $K \vee H$ is finite for any finite subgroups K, H of G. Give a counterexample showing that the above statement is false without the assumption that G is abelian.

3. Show that a group that has only a finite number of subgroups must be finite.

4. Show that if H and K are subgroups of a finite group G such that $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.

5. Let K, H, G be groups with $K \lhd H \lhd G$.

   (a) Prove that if H is cyclic, then $K \lhd G$.

   (b) Give an example of G, H, K such that $K \lhd H \lhd G$ but K is not normal in G.

6. Let G be a finite group.

   (a) Prove that if $|G| = 30$, then G is not simple.

   (b) Prove that if $|G| = 96$, then G is not simple.

7. Let R be a commutative ring with identity and prime characteristic p and let n be a positive integer. Show that the map $R \to R$ given by $r \mapsto r^{p^n}$ is a homomorphism of rings.

8. Let $\mathbb{Q}$ be the field of rational numbers and R any ring. Show that if $f, g : \mathbb{Q} \to R$ are homomorphisms of rings such that the restrictions of f and g to $\mathbb{Z}$ are equal ($f|\mathbb{Z} = g|\mathbb{Z}$), then $f = g$.

9. Let F be an extension field of a field K, and $u_1, \ldots, u_n \in F$. Prove that the field $K(u_1, \ldots, u_n)$ is isomorphic to the field of fractions of the ring $K[u_1, \ldots, u_n]$.

10. Let F be an extension field of a field K, and let $u \in F$. Prove that if u is algebraic of odd degree over K, then u^2 is also algebraic of odd degree over K and $K(u) = K(u^2)$.

11. Let F be an extension field of a field K, and let $u, v \in F$. Prove that if v is algebraic over $K(u)$ and it is transcendental over K, then u is algebraic over $K(v)$.

12. Let F be an algebraic field extension of a field K and D be a ring with $K \subseteq D \subseteq F$. Prove that D is a field.

13. Let $F = \mathbb{Q}(i, \sqrt{3}, \omega)$, where $i \in \mathbb{C}$, $i^2 = -1$, and ω is a complex (nonreal) cube root of 1. Find $[F : \mathbb{Q}]$ and a basis of F over $\mathbb{Q}$.

14. Construct a field with 8 elements (write both the addition and the multiplication tables).

15. Let $R = \{a+b\sqrt{2}|a, b \in \mathbf{Z}\}$ be a subring of the reals. Then R can be considered either as a $\mathbb{Z}$-module or as an R-module. Let $f : R \to R$ be given by $f(a + b\sqrt{2}) = a + b$. Prove or disprove each of the following:

    (a) f is a $\mathbb{Z}$-homomorphism;

    (b) f is an R-homomorphism.

16. Let $f : A \to A$ be an R-module homomorphism such that $f \circ f = f$. Prove that A is isomorphic to the direct sum $\ker f \oplus \operatorname{Im} f$.

17. Let R be a commutative ring and A be an R-module. An element $a \in A$ is a *torsion element* of A iff there is a nonzero $r \in R$ such that $ra = 0$. Prove that if R is an integral domain, then the set $T(A)$ of all torsion elements of A is a submodule of A, and give an example of a commutative ring R and an R-module A such that $T(A)$ is not a submodule of A.

Ph.D. Entrance Examination in Algebra

April 2001

Directions: Work any ten problems. If you turn in partial solutions to more than 10 problems, indicate clearly which 10 should be graded.

1. Let G be the group of order pq, where p and q are two distinct prime numbers. Show each of the following:

(i) G has an element a with $|a| = p$ and an element b with $|b| = q$.

(ii) G is a cyclic group.

2. Let $\mathbf{Z}$ denote the ring of all integers with the usual addition and multiplication.

(i) Show that the integral domain $\mathbf{Z}$ is a principal ideal domain.

(ii) Is it possible to write $\mathbf{Z}$ as a union of three proper principal ideals?

(iii) Is it possible to write $\mathbf{Z}$ as a union of two proper principal ideals?

3. Let H, K, N be subgroups of a group G such that H is a subgroup of K. Show that the following are equivalent.

(i) $H = K$.

(ii) $H \cap N = K \cap N$ and $HN = KN$.

4. Prove that there is no simple group of order 105.

5. Show that if N is a normal subgroup of G with $[G : N]$ finite, and if H is a finite subgroup of G such that $[G : N]$ and $|H|$ are relatively prime, then H is a subset of N.

6. Draw the lattice of all of the intermediate fields between $\mathbf{Q}$ and $\mathbf{E}$, the splitting field of $x^4 - 2$ over $\mathbf{Q}$. Find $\mathrm{Gal}(\mathbf{E}/F)$ for each of these intermediate fields F.

7. $R = \{a + b\sqrt{2} | a, b \in \mathbf{Z}\}$ is a subring of the reals. R can be considered either as a $\mathbf{Z}$ module or as an R-module. The map $f : R \to R$ is given by $f(a + b\sqrt{2}) = a + b$. prove or disprove each of the following:

(i) f is a $\mathbf{Z}$-homomorphism.

(ii) f is an R-homomorphism.

8. Let R be a ring and $f : A \longrightarrow B$ be an R-module homomorphism, and C be an R-submodule of $Ker(f)$. Prove the following (The first isomorphism theorem of R-module homomorphism.)

(i) There is a unique R-module homomorphism $\tilde{f} : A/C \longrightarrow B$ such that $\tilde{f}(a + C) = f(a)$, $\forall a \in A$; $Im(\tilde{f}) = Im(f)$ and $Ker(\tilde{f}) = Ker(f)/C$.

(ii) $\tilde{f}$ is an isomorphism if and only if f is an R-module epimorphism and $C = Ker(f)$.

(iii) $A/Ker(f) \equiv Im(f)$.

9. An R-module M is called irreducible if it has no nontrivial submodules. Prove that if M is an irreducible R-module then every R-module homomorphism $f : M \to M$ is either an isomorphism or the zero map.

10. Let G' denote the commutator subgroup of G. If N is a normal subgroup of G such that $N \cap G' = \{e\}$ (where e is the identity of G), then $N \subseteq C(G)$, (where $C(G)$ is the center of G).

11. If a group G has an element a with exactly two conjugates, then G has a proper normal subgroup N with at least two elements.

12. If H is a subgroup of G with $|G : H| < \infty$, show that there is only a finite number of distinct subgroups in G of the form aHa^{-1}, where $a \in G$.

13. Prove that $\mathbf{Q}(\sqrt{3} + \sqrt{5}) = \mathbf{Q}(\sqrt{3}, \sqrt{5})$.

14. Let G be a group of order p^n for some prime p and positive integer n. Show that if k is an integer with $0 \leq k \leq n$, then G has a normal subgroup of order p^k.

15. Let K be an extension field of F, and let $s, t_1, t_2, ..., t_n$ be elements in K. Show that s is algebraically dependent on $\{t_1, t_2, ..., t_n\}$ over F if and only if there exist a finite number of polynomials $a_i(x_1, x_2, ..., x_n) \in F[x_1, x_2, ..., x_n]$ such that

$$\sum_{i \geq 0} a_i(t_1, t_2, ..., t_n) s^i = 0.$$