1966 Ph.D. Qualifying Examination

ALGEBRA

INSTRUCTIONS

There are four parts numbered I - IV. Answer a total of ten questions selecting at least two but not more than three questions from any one part. Each question counts 10 points.

For each question selected, use a separate blue book. Write your name, the part number and the question number on the cover of the blue book.

NOTATION

$\mathbb{Z}_n$ = cyclic group of order n ;

$\mathbb{Z}$ = integers;

$\mathbb{Q}$ = rationals;

$\mathbb{R}$ = reals;

$\mathbb{C}$ = complexes;

$\mathbb{F}_q$ = the Galois field of q-elements where $q = p^n$, p a prime.

Algebra

PART II. RINGS

1. Let D be an integral domain. Explain the following notions and their basic relationships:

   (a) D is a unique factorization domain.

   (b) D is a principal ideal domain.

   (c) D satisfies the ascending chain condition for ideals.

2. In a commutative ring with unity, show that the intersection of all prime ideals is the set of all nilpotent elements.

3. Show that the polynomial ring $\mathbb{Z}[x]$ is Noetherian. Further, let $n(I)$ = the minimal number of generators of an ideal I of $\mathbb{Z}[x]$. Is $n(I)$ bounded?

4. Prove that a commutative ring A can be extended to a commutative ring B such that all non-zero divisors in A are units in B.

5. Let R be a ring. For any subring S of R let $C(S)$ be the set of all elements of R which commute with each element of S. Prove that $C(C(C(S))) = C(S)$. Can this be strengthened to $C(C(S)) = S$?

ALGEBRA

PART I. GROUPS.

1. Let G be a group, and let $G^{(2)}$ be the subgroup of G generated by all squares. Prove that $G^{(2)}$ contains the commutator subgroup of G .

2. Find the characteristic subgroups of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$. (Characteristic means invariant under all automorphisms.)

3. State and explain the Isomorphism Theorems, and briefly show how they apply to the Jordan-Hölder Theorem.

4. Give with proof an example of an infinite simple group.

5. Let G be a finite group, and let $H \subset G$ be a proper subgroup. Prove that G is not the union of the conjugate subgroups of H .

PART III. FIELDS.

1. Suppose K is a field and G is a finite subgroup of $K - \{0\}$ under multiplication. Prove that G is cyclic.

2. a) Suppose ζ is a primitive n^{th} root of unity, p is a prime not dividing n, and that ζ is a root of a monic polynomial $f(x)$ irreducible over $\mathbb{Q}$. Show that $f(\zeta^p) = 0$.

   b) Prove that if $\Phi_n(x) = \prod (x-\zeta)$ (where the product runs over all primitive n^{th} roots of unity), then the polynomial $\Phi_n(x) \in \mathbb{Q}[x]$ and is irreducible over $\mathbb{Q}$.

3. Let K be a field, and let $f(x) \in K[x]$ be a polynomial without double roots. Show that $f(x)$ is irreducible over K iff the Galois group of $f(x)$ is transitive on the roots of f.

4. Let α be a rational number which is not a 3rd power. Find the degree of the splitting field of $x^3-\alpha$ over $\mathbb{Q}$.

5. If p is a prime, how many subfields of $\mathbb{F}_{p^n}$ are there? Prove your assertion.

There are 5 parts, to be scored seperately as follows:

I - 30% , II - 20% , III - 20% , IV - 10% , V - 20% .

Instructions as to the possible choices are provided seperately with each part. Indicate clearly on the cover of your test book(s) which sections you have chosen. Notation: $\mathbb{Z}$ = integers, $\mathbb{Q}$ = rationals, $\mathbb{R}$ = reals, $\mathbb{C}$ = complex numbers; D[x] = ring of polynomials in x over D .

I. Miscellaneous (30%). Do each of (1) - (6).

In each of the cases where a true (T) or false (F) answer is demanded, give a brief justification of your answer.

(1) (T or F) If a is in Z and is not a perfect cube, then the order of the Galois group of the polynomial x^3-a over Q is 6 .

(2) Define the following notions, where $K \subseteq L_1 \subseteq N$ are fields:

(a) L_1 is a finite extension of K ; (b) N is a normal extension of K ; (c) L_1 and L_2 are conjugate relative to K.

(3) (T or F) If A and B are any two sets of transcendental real numbers of the same cardinality then there is an automorphism of the field $\mathbb{C}$ which maps A into B .

(4) (T or F) In any principal ideal domain every prime ideal is maximal.

(5) Define what is meant by the characteristic polynomial of T , where T is a linear transformation of a finite dimensional vector space. State the Cayley - Hamilton theorem.

(6) (T or F) If G is a finite group and $g \in G$ then the number of conjugates of g is a divisor of the order of G.

<u>In each of the following parts a proof of the assertion is required.</u> <u>Each is scored 10%</u>.

II. <u>Group Theory</u> Do either (1)(a) <u>or</u> (1)(b) <u>and</u> either (2)(a) <u>or</u> (2)(b).

(1) (a) If p is prime and G is a group of order p^2 then G is Abelian.

(b) Any group of order 15 is cyclic.

(2) (a) Every subgroup of a finitely generated free Abelian group is free.

(b) Prove the Jordan-Hölder theorem for finite groups by induction on the order, without using the Schreier refinement theorem.

III. <u>Domains and fields</u> Do either (1)(a) <u>or</u> (1)(b) <u>and</u> (2)(a) <u>or</u> (2)(b).

(1) (a) Suppose K is an algebraically closed extension of $\mathbb{Q}$; an element α of K is said to be an algebraic integer if for some monic $f(x) \in \mathbb{Z}[x]$, $f(\alpha) = 0$. Then if α, β are algebraic integers so also is $\alpha+\beta$.

(b) Suppose D is a unique factorization domain and K its field of quotients. Then if $f(x) \in D[x]$ and is irreducible over D, it continues to be irreducible over K.

(2) (a) Suppose K is a finite field, $f(x) \in K[x]$ of non-zero degree, and that N is a splitting field (root field) of $f(x)$ over K. Then the Galois group of $f(x)$ over K is transitive on the set of roots of $f(x)$ if and only if $f(x)$ is irreducible over K.

(b) If K is a field and G is a finite subgroup of the multiplicative group $K - \{0\}$ then G is cyclic.

IV. Ideals Do (1)(a) or (1)(b). In both parts assume that R is any commutative ring with unity.

(1) (a) If P is a primary ideal in R, and A,B are ideals with $AB \subseteq P$ and B is finitely generated then $A \subseteq P$ or for some $m > 0$, $B^m \subseteq P$.

(b) If A is an ideal in R then there exists a minimal element in the class of all prime ideals P such that $A \subseteq P$.

V. Linear Algebra Do (1)(a) or (1)(b) and (2). In each case V is assumed to be a finite-dimensional vector space over a field K.

(1) (a) Let V^* be the dual space of V and for any subspace U of V, let $A(U)$ be the annihilator of U in V^*. Then:

(i) V^* is finite-dimensional (over K) with the same dimension as V, and (ii) if U is a subspace of V then $U^* \cong V^* / A(U)$.

(b) A linear transformation T of V is called a projection if for some U_1, U_2, $V = U_1 \oplus U_2$ and $T(u_1 + u_2) = u_1$ for all $u_i \in U_i$. Then

(i) for any linear transformation T of V, T is a projection if and only if $T^2 = T$;

(ii) for any linear transformation T of V, there exists a non-singular linear transformation T_1 of V such that $T_1 T$ is a projection.

(V (2) See page 4)

V (2) Assume $K = \mathbb{C}$ and that V is an inner product space, i.e. we have a function (u,v) on $V \times V$ into $\mathbb{C}$, linear in u, with $(u,v) = \overline{(v,u)}$, $(u,u) \geq 0$ and $(u,u) = 0$ if and only if $u = 0$. Assume standard results on the existence of orthonormal bases.

(i) For each linear transformation T of V there is a unique w such that for all $u \in V$, $(T(u),v) = (u,w)$.

(ii) Define $T^*: V \to V$ by $(T(u),v) = (u,T^*(v))$ for all u,v; then T is linear.

(iii) T is called self-adjoint if $T^* = T$. If T is self-adjoint then all its eigenvalues are real.