QUALIFYING EXAM IN ALGEBRA

AUGUST 1991

1. Work as many problems as you can. It is to your advantage to demonstrate a broad background.

2. If you feel there is a misprint or error in the statement of the problem, then interpret it in such a way that the problem is not trivial.

Group Theory

1. How many elements of order 6 are there in S_6? How many in A_6?

2. Let H be a subgroup of a group G, $C_G(H)$ the centralizer of H in G, and $N_G(H)$ the normalizer of H in G. Show the following:
   (a) $C_G(H)$ is a normal subgroup of $N_G(H)$.
   (b) $N_G(H)/C_G(H)$ is isomorphic to a subgroup of the automorphism group of H.

3. Let H, K be subgroups of a group G, with $K \subseteq H$ and K a normal subgroup of G. Let $[H, G]$ be the subgroup of G generated by $\{\, h^{-1}g^{-1}hg \mid h \in H,\ g \in G \,\}$. Show that if H/K is contained in the center of G/K, then $[H, G] \subseteq K$.

4. Let G be a cyclic group of order 12 with generator a. Find b in G such that $G/\langle b \rangle$ is isomorphic to $\langle a^{10} \rangle$. (Here $\langle x \rangle$ denotes the subgroup of G generated by $\{x\}$, for $x \in G$.)

5. Show that a group of order $2001 = 3 \cdot 23 \cdot 29$ must contain a normal cyclic subgroup of index 3.

6. Let G be a finite simple group and p a prime such that p^2 divides the order of G. Show that G has no subgroup of index p.

7. Let p be a prime and G a nonabelian group of order p^3.
   (a) Show that $Z(G)$, the center of G, has order p.
   (b) Show that G', the commutator subgroup of G, is equal to $Z(G)$.
   (c) Show that $G/Z(G)$ is isomorphic to $\mathbf{Z}_p \times \mathbf{Z}_p$.

Ring Theory

1. Give an example of each of the following.

   (a) An irreducible polynomial of degree 3 in $\mathbf{Z}_3[x]$.

   (b) A noncommutative ring of characteristic p, p a prime.

   (c) A ring with exactly 6 invertible elements.

2. Denote the set of invertible elements of the ring $\mathbf{Z}_n$ by U_n.

   (a) List all the elements of U_{24}.

   (b) Is U_{24} a cyclic group under multiplication? Justify your answer.

3. Let R be a commutative ring with idenity.

   (a) Prove that (x) is a prime ideal in $R[x]$ if and only if R is an integral domain.

   (b) Prove that (x) is a maximal ideal in $R[x]$ if and only if R is a field.

   (c) Give an example of a commutative ring R which has an non-zero prime ideal that is not a maximal ideal.

4. Let $D = \mathbf{Z}(\sqrt{5}) = \{\, m + n\sqrt{5} \mid m, n \in \mathbf{Z} \,\}$ — a subring of the field of real numbers and necessarily an integral domain (you need not show this) — and $F = \mathbf{Q}(\sqrt{5})$ its field of fractions. Show the following:

   (a) $x^2 + x - 1$ is irreducible in $D[x]$ but not in $F[x]$.

   (b) D is not a unique factorization domain.

5. Let D be an integral domain and F its field of fractions. Let P be a prime ideal in D and $D_P = \{\, ab^{-1} \mid a, b \in D,\ b \notin P \,\} \subseteq F$. Show that D_P has a unique maximal ideal.

6. Let R be a commutative ring with identity and let S be the set of all elements of R that are *not* zero-divisors. Show that there is a prime ideal P such that $P \cap S$ is empty. (Hint: Use Zorn's Lemma.)

Field Theory

1. Let F be a field with the property

   (*) If $a, b \in F$ and $a^2 + b^2 = 0$, then $a = 0$ and $b = 0$.

   (a) Show that $x^2 + 1$ is irreducible in $F[x]$.

   (b) Which of the fields $\mathbf{Z}_3$, $\mathbf{Z}_5$ satisfy (*)?

2. Let K be a field extension of F of degree n and let $f(x) \in F[x]$ be an irreducible polynomial of degree m, where m is relatively prime to n. Show that $f(x)$ has no root in K.

3. Let x and y be independent indeterminates over $\mathbf{Z}_p$, $K = \mathbf{Z}_p(x, y)$, and $F = \mathbf{Z}_p(x^p, y^p)$.

   (a) Show that $[K : F] = p^2$

   (b) Show that K is not a simple extension of F.

4. Let η be a complex primitive 7-th root of unity and let $K = \mathbf{Q}(\eta)$. Find $\mathrm{Gal}(K/\mathbf{Q})$ and express each intermediate field F between K and $\mathbf{Q}$ as $F = \mathbf{Q}(\beta)$ for some $\beta \in K$.

5. (a) Determine the Galois group of $x^4 - 4$ over the field $\mathbf{Q}$ of rational numbers.

   (b) How many intermediate fields are there between $\mathbf{Q}$ and the splitting field of $x^4 - 4$ (including $\mathbf{Q}$ and the splitting field)?

6. Show that every finite extension of a finite field is a Galois extension.

Linear Algebra

1. Let V be a finite dimensional vector space and $T : V \to V$ a linear transformation.

   (a) Show that T is invertible if and only if the minimal polynomial of T has non-zero constant term.

   (b) Show that if T is invertible, then T^{-1} is expressible as a polynomial in T.