August 1999
Algebra Qualifying Exam

1A) An $n \times n$ matrix A over a field F is called anti-idempotent if $A^2 = -A$. Suppose A is anti-idempotent.

(a) What are the possible minimal polynomials for A?

(b) Show that A is diagonalizable over F.

(c) Show that two idempotent matrices over F are similar if and only if they have the same rank.

1B) Let α be $\sqrt{2} + \sqrt{-1}$ in $\mathbb{Q}\left(\sqrt{2}, \sqrt{-1}\right) = L$. Choose a $\mathbb{Q}$-basis B for the $\mathbb{Q}$-vector space L. Furthermore, determine the matrix M_B of the linear transformations $\alpha^* : L \to L$ given by $x \to x \cdot \alpha$ and the rational canonical form of M_B.

2A)There is a simple group of order 168. Determine, with reasons, how many elements of order 7 it has.

2B) Let G be a finite nilpotent group. Show that for any divisor n of the order of G there exists a subgroup whose order is n. Hint: Consider the case that G is a p-group, p a prime first. Note that the center of G is nontrivial.

3A) Suppose the abelian group A has presentation

$$A = \langle a, b, c, d : 3a = 7d, b = 3d, 2a = b - 5d \rangle$$

Determine the structure of A as a direct sum of cyclic groups.

3B) Let R be a PID, let M be a free R-module of finite rank and let f be an R-endomorphism of M. Show that f is injective if and only if $M/\operatorname{Im}(f)$ is an R-torsion module.

4A) Recall that two elements r and s of a ring R are algebraically independent over a subring S of R is the only poynomial $f(x, y) \in S[x, y]$ for which $f(r, s) = 0$ is the zero polynomial. If p and q are distinct (positive) primes in $\mathbb{Z}$, show that $\sqrt{p}$ and $\sqrt{q}$ are algebraically independent over $\mathbb{Z}$. **Note:** This is not true, find a counterexample.

4B) Let $f(x) = x^3 + 5x - 1 \in \mathbb{Q}[x]$.

(a) Show that f is an irreducible polynomial over $\mathbb{Q}$.

(b) Since f is irreducible $L = \mathbb{Q}[x]/(f)$ is a field. Determine the multiplicative inverse of $2x - 2 + (f)$ in L explicitly.

5A) Let $F = C$, let $K = C(t)$, the field of rational operatornametions is an indeterminate t, and let G *be* the Galois group $G(K : F)$. Suppose φ and θ in G are determined by $\varphi(t) = \zeta t$ and $\theta(t) = 1/t$, where ζ is a primitive n^{th} root of unity in C, $n \geq 4$, and set $H = \langle \varphi, \theta \rangle \leq G$. Show that H is isomorphic with the dihedral group of order $2n$.

5B) Let $\mathbb{F}_n$ denote the field with n elements.

(a) Construct explicitly the field with 64 elements by taking a degree 3 irreducible polynomial in $\mathbb{F}_4$.

(b) Determine the order and structure of the Galois group G of this extension.

(c) How many primitive elements over $\mathbb{F}_4$ does $\mathbb{F}_{64}$ contain? Justify.