DEPARTMENT OF MATHEMATICS
University of Toronto

Algebra Exam
May 2001

Time: 3 hours — No aids allowed

1. *[20 points]*

a) Define p-group, and Sylow p-subgroup for a finite group.

b) State Sylow's Theorem.

c) Let P be a cyclic p-group for some prime p. Determine the order of the automorphism group $\mathrm{Aut}(P)$ of P.

d) Let p be the smallest prime dividing the order of a finite group G. Prove that if P is a Sylow p-subgroup of G and P is cyclic, then the centralizer $C_G(P)$ of P in G is equal to the normalizer $N_G(P)$ of P in G.

2. *[20 points]*

Let T be the linear transformation on the complex vector space

$$V = \mathbb{C}[x]/(x^2-4)(x+2) \oplus \mathbb{C}[x]/(x^4-16) \oplus \mathbb{C}[x]/(x^2+4)^2(x-2)$$

obtained by multiplying by x.

a) Find the invariant factors and elementary divisors of T.

b) Determine the rational canonical form and the Jordan canonical form of T.

c) Find the minimal and characteristic polynomials of T.

3. *[20 points]*

Let R and S be commutative rings with 1.

a) Give the definitions of a prime ideal in R, a primary ideal in R, and the radical $\mathrm{Rad}(I)$ of an ideal I in R.

Let $f : R \to S$ be a surjective ring homomorphism. Let $J \subset S$ be an ideal. Set $I = f^{-1}(J)$.

b) Show that J is prime in S if and only if I is prime in R.

c) Show that J is primary in S if and only if I is primary in R.

d) Show that if $P = \mathrm{Rad}(J)$, then $f^{-1}(P) = \mathrm{Rad}(I)$.

4. *[20 points]*

Let R be a commutative ring with 1.

a) Define cyclic R-module and simple R-module.

b) Show that if M is a cyclic R-module, then $M \simeq R/I$ for some ideal I in R.

c) Assume that R is an integral domain. Define principal ideal domain and prove that R is a principal ideal domain if and only if every cyclic R-module has the property that each of its R-submodules is cyclic.

5. *[20 points]*

a) Define field, field extension, separable field extension, finite Galois extension, and Galois group of a finite Galois extension.

b) State the fundamental theorem of Galois theory.

Recall that a finite extension K' of a field K is said to be abelian if K' is Galois over K and the Galois group $\mathrm{Gal}(K'/K)$ is abelian. Let L be a finite (not necessarily abelian) Galois extension of a field K with Galois group $\mathrm{Gal}(L/K)$.

c) Prove that there exists a unique maximal abelian intermediate extension K^{ab} of K contained in L. That is, show that there exists an extension K^{ab} of K contained in L such that K^{ab} is an abelian extension of K and any abelian extension K' of K contained in L must actually be contained in K^{ab}. (*Hint*: If K^{ab} exists, what are the properties of $\mathrm{Gal}(L/K^{ab})$?)