UNIVERSITY OF WATERLOO

Department of Pure Mathematics

Algebra Comprehensive Examination **Winter 2011**

Examiners: Barbara Csima, Frank Zorzitto

Answer as many questions as you can. It is important to demonstrate comprehensive knowledge in each of the four areas: linear algebra, group theory, ring theory and field theory.

Linear Algebra

[10] L1. If $T : V \to V$ is a linear operator on an n-dimensional vector space and the characteristic polynomial of T splits into linear factors, prove that T can be represented by an upper triangular matrix using a suitable basis of V. Your proof should be elementary and not use advanced results such as the Jordan canonical form.

[5] L2. If A is a 3×3 matrix over the complex numbers and $\text{trace}(A^k) = 0$ for $k = 1, 2, 3$, prove that $A^3 = 0$.

[15] L3. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be a linear transformation such that $\|Tx\| = \|x\|$ for all x in $\mathbb{R}^3$, and such that $\det T = 1$.

(a) Show that 1 is an eigenvalue of T.

(b) If V is the eigenspace for the eigenvalue 1, show that $V^{\perp}$ is T-invariant.

(c) Show that with respect to a suitable orthonormal basis of $\mathbb{R}^3$ the operator T has a matrix representation of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

for some number θ.

(d) If two operators S, T each have a matrix representation of the above type, not necessarily with respect to the same orthonormal basis, does their composite ST also have a representation of the above type?

Group theory

[5] G1. Use the Sylow theory to show that every group of order 100 has a non-trivial normal subgroup.

[5] G2. Letting $\mathbb{Z}_n$ denote the cyclic group of order n, sort the following abelian groups into isomorphism classes:

$$\mathbb{Z}_{25} \times \mathbb{Z}_4,\ \mathbb{Z}_{90},\ \mathbb{Z}_{100},\ \mathbb{Z}_3 \times \mathbb{Z}_{30},\ \mathbb{Z}_9 \times \mathbb{Z}_{10},\ \mathbb{Z}_{10} \times \mathbb{Z}_{10},\ \mathbb{Z}_{50} \times \mathbb{Z}_2.$$

[5] G3. Let G be a finite group acting on a finite set X. If $p \in X$, the orbit of p is the subset of X given by:

$$O_p = \{\sigma p : \sigma \in G\}.$$

The stabilizer of p is the subset of G given by:

$$S_p = \{\sigma \in G : \sigma p = p\}.$$

Show that the cardinality of G is the product of the cardinality of O_p and the cardinality of S_p.

[15] G4. This problem is about p-groups, i.e. groups of order p^e where p is a prime and e is a positive integer.

(a) Prove that a p-group has a non-trivial centre.

(b) Identify all groups of order p^2, up to isomorphism, and justify your answer.

(c) If $e \geq 2$, prove that groups of order p^e are nilpotent of class at most $e - 1$.

Ring theory

[5] R1. Prove that every homomorphic image of a left Noetherian ring is again left Noetherian.

[5] R2. If $\langle X^2 + 1 \rangle$ is the ideal generated by $X^2 + 1$ in the polynomial ring $\mathbb{C}[X]$, prove that $\mathbb{C}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C} \times \mathbb{C}$.

[5] R3. If $\mathbb{Z}[X]$ is the ring of polynomials in X with integer coefficients and $\langle X^2+1, X-2\rangle$ is the ideal generated by the polynomials indicated, prove that the quotient ring $\mathbb{Z}[X]/\langle X^2+1, X-2\rangle \cong \mathbb{Z}_5$, the finite field of residues modulo 5.

[15] R4. In this problem R is an integral domain.
An element p in R is called *prime* provided p is not a unit, and

$$a, b \in R \text{ and } p|ab \implies p|a \text{ or } p|b.$$

A subset D of R is called *multiplicatively closed* provided $1 \in D$, and

$$a, b \in D \implies ab \in D.$$

The set D is called *saturated* provided

$$ab \in D \implies \text{both } a \in D \text{ and } b \in D.$$

(a) If R is a unique factorization domain, show that every non-zero prime ideal contains a prime element.

(b) Prove that the complement of a union of prime ideals in R is a multiplicatively closed and saturated set.

(c) If D is a multiplicatively closed and saturated set in R and $x \in R \setminus D$, show that R contains an ideal P such that $x \in P$, $P \cap D = \emptyset$ and P is maximal with respect to these properties.

(d) Continuing with item (c), show that the ideal P is a prime ideal.

(e) If R is not a unique factorization domain, show that there is a non-zero prime ideal P inside R such that P contains no prime element.
Hint. The set D of elements in R that are either units or products of primes is multiplicatively closed and saturated.

Field theory

[15] F1. Let $\alpha = \sqrt[3]{5}$, the real cube root of 5, and $\beta = \sqrt{-3}$, a complex square root of -3.

(a) Find the degree of the field extension $\mathbb{Q}(\alpha, \beta)$ over $\mathbb{Q}$, and justify your answer.

(b) Show that the extension $\mathbb{Q}(\alpha, \beta)$ is the splitting field of the polynomial $X^3 - 5$ over $\mathbb{Q}$.

(c) List all the elements of the Galois group of the extension $\mathbb{Q}(\alpha, \beta)$. It suffices to specify the group actions only on the field generators α, β. Explain why every action of the Galois group must appear on your list, and why your list picks up the entire Galois group.

(d) Display the lattice of subfields of the extension $\mathbb{Q}(\alpha, \beta)$, and show that all subfields have been included.

[15] F2. (a) If a field K is a finite extension of an infinite field F and there are only a finite number of intermediate subfields, show that $K = F(\theta)$ for some θ in K.

(b) If θ is an algebraic element over a field F, show that there are only finitely many fields between F and the field extension $F(\theta)$.