The University of Melbourne

Semester 1 Assessment 2008

Department of Mathematics and Statistics
620-321 Algebra

Reading Time: 15 minutes.
Writing Time: 3 hours.
This paper has: 3 pages.

Identical Examination Papers: None.
Common Content Papers: None.

Authorised Materials:
Pens, pencils, rubbers, rulers. No other materials are authorised. Calculators and mathematical tables are not permitted. Candidates are reminded that no written or printed material related to this subject may be brought into the examination. If you have any such material in your possession, you should immediately surrender it to an invigilator.

Instructions to Invigilators:
Each candidate should be issued with an examination booklet, and with further booklets as needed. The students may remove the examination paper at the conclusion of the examination.

Instructions to Students:
This examination consists of 9 questions. All questions may be attempted. Answers should be appropriately justified. The number of marks for each question is approximately the same (even though the amount of work or sophistication may vary substantially). All of your calculations and working should be shown.

This paper may be held by the Baillieu Library.

— BEGINNING OF EXAMINATION QUESTIONS —

1. (a) Give the definitions of integral domain and field.

   (b) (i) Give an example of a commutative ring with multiplicative identity that is not an integral domain.

   (ii) Give an example of an integral domain that is not a field.

   (c) Show that every finite integral domain is a field.

2. (a) Let $f, g \in \mathbb{Q}[x]$ be given by

$$f(x) = x^5 + 3x^4 + x^3 + x^2 + 3x + 1 \quad \text{and} \quad g(x) = x^4 + 2x^3 + x + 2.$$

   Use the Euclidean algorithm to find polynomials $u, v \in \mathbb{Q}[x]$ such that $uf + vg$ is a greatest common divisor of f and g.

   (b) Show that $\gcd(x^m - 1, x^n - 1) = x^d - 1$, where $d = \gcd(m, n)$.

3. (a) Show that the following are irreducible in $\mathbb{Q}[x]$:

$$x^2 + x + 1, \quad x^3 + 7x + 7, \quad x^4 + x + 1.$$

   (b) Write the following as a product of irreducibles in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ and $\mathbb{Z}_2[x]$:

$$3x^6 + 3x^5 + 3x^4 + 3x^3 + 3x^2 + 3x + 3$$

   (c) Let R be a PID, and $p \in R$ a non-zero, non-unit element. Show that p is irreducible if and only if (p) is a maximal ideal in R. Give an example to show that this result does not always hold in a UFD.

4. (a) State the Structure Theorem for finitely generated modules over a PID.

   (b) List, up to isomorphism, all abelian groups of order 360. Give the primary decomposition and annihilator (as a $\mathbb{Z}$-module) of each group.

5. Let R be a commutative ring with identity.

   (a) What does it mean to say that an R-module is free?

   (b) Show that every finitely generated R-module is isomorphic to a quotient of a free R-module.

   (c) Let F be the $\mathbb{Z}$-module $F = \mathbb{Z}^4$ and let N be the submodule of F generated by

$$\{(1, 1, 1, 1), (1, -1, 1, -1), (1, 3, 1, 3)\} \subset \mathbb{Z}^4.$$

   Give a direct sum of non-trivial cyclic $\mathbb{Z}$-modules that is isomorphic to F/N.

6. Let $A \in M_7(\mathbb{C})$ be a matrix and suppose that the invariant factors of the matrix $xI - A \in M_7(\mathbb{C}[x])$ are: $1, 1, 1, 1, x, x(x-i), x(x-i)^3$.

   (a) Give the corresponding decomposition of $\mathbb{C}^7$ regarded as a $\mathbb{C}[x]$-module. (All summands should be non-trivial cyclic $\mathbb{C}[x]$-modules.)

   (b) Give the Jordan Normal Form of the matrix A.

   (c) Give the minimal and characteristic polynomials of A.

   (d) Is A diagonalizable?

7. (a) Let F be a finite field of characteristic p. Show that the number of elements in F is p^r, for some $r \in \mathbb{N}$.

   (b) Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

      (i) Calculate $[E : \mathbb{Q}]$.

      (ii) Find an element $a \in E$ for which $E = \mathbb{Q}(a)$.

8. (a) (i) Suppose that $a \in \mathbb{R}$ is a constructible number. What can be said about the degree of a over $\mathbb{Q}$.

      (ii) Explain why it is not possible to construct, with straight-edge and compass, a circle of radius r, if $r \in \mathbb{R}$ is a root of the polynomial $x^3 + 3x + 1$.

   (b) Show that the set of real numbers that are algebraic over $\mathbb{Q}$ is a subfield of $\mathbb{R}$.

9. (a) Find the Galois group of the extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$ of $\mathbb{Q}$, explain why it is a Galois extension and list the correspondence between subgroups of $G(K/\mathbb{Q})$ and subfields $\mathbb{Q} \subseteq L \subseteq K$.

   (b) Let K be the splitting field of the polynomial $f(x) = x^3 - 2$.

      (i) Calculate $[K : \mathbb{Q}]$.

      (ii) Find a basis for K as a $\mathbb{Q}$-vector space.

      (iii) Identify the Galois group $G(K/\mathbb{Q})$, and identify it.

      (iv) Write down a field L such that $\mathbb{Q} \subseteq L \subseteq K$ and L is not a Galois extension of $\mathbb{Q}$.

— END OF EXAMINATION QUESTIONS —