THE UNIVERSITY OF BRITISH COLUMBIA
SESSIONAL EXAMINATIONS – APRIL 2014
MATHEMATICS 323

Time: 2 hours 30 minutes

Instructions: Total number of points: 100.

The mark for the exam will be based on Question 1 and the best 4 of the remaining questions. That is, you need to do only Question 1 and any 4 of the remaining ones (provided you do them correctly) for full marks.

You can use the statements we proved in class, or the theorems proved in the textbook, without proof; but you need to provide complete statements of all the results you quote.

Write your name and student number at the top of each booklet you use, and please number the booklets (e.g. "booklet 2 of 5") if you use more than one.

---

1. Mandatory question [40 points] (each sub-part is 4 points).

Determine whether the following statements are **True** or **False** (you have to include short proofs/counterexamples):

(1) (a) Any prime ideal of $\mathbb{Z}[x]$ is maximal.
(b) Any maximal ideal of $\mathbb{Z}[x]$ is prime.

(2) The polynomial $f(x) = x^7 + 15x^5 - 75x^4 + 20x - 10$ is irreducible in $\mathbb{Z}[x]$.

(3) (a) The rings $\mathbb{Z}[x]/(x^2+1)$ and $\mathbb{Z}[x]/(x^2+2)$ are isomorphic.
(b) The $\mathbb{Z}$-modules $\mathbb{Z}[x]/(x^2+1)$ and $\mathbb{Z}[x]/(x^2+2)$ are isomorphic.
(c) The $\mathbb{Z}[x]$-modules $\mathbb{Z}[x]/(x^2+1)$ and $\mathbb{Z}[x]/(x^2+2)$ are isomorphic.

(4) Let R be an integral domain. Let F be a free module over R, and let M be an arbitrary R-module.
(a) There always exists a non-zero module homomorphism from F to M.
(b) There always exists a non-zero module homomorphism from M to F.

(5) Recall that a module M over an integral domain R is called *torsion* if for every element $m \in M$ there exists $r \in R$, $r \neq 0$, such that $r \cdot m = 0$.
(a) Any finitely generated module over $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a direct sum of a free module and a torsion module.
(b) Any finitely generated module over $\mathbb{Z}[\sqrt{-3}]$ is a direct sum of a free module and a torsion module.

The following questions are 15 points each. You only need to do any 4 of them for full marks.

2. (a) Show that $x^4 + 2$ is irreducible in $\mathbb{F}_5[x]$.
(b) Describe the quotient $\mathbb{F}_5[x]/(x^4+2)$.
(c) Show that $f(x) = x^4 + 5x^2 - 3$ is irreducible in $\mathbb{Q}[x]$.

3. (a) Prove that $\mathbb{F}_5[x]/(x^3+x+1)$ is a field of 125 elements (denote it by $\mathbb{F}_{125}$).
(b) Let α be a root of the polynomial $f(x) = x^3 + x + 1$ in $\mathbb{F}_{125}$. Prove that every element of $\mathbb{F}_{125}$ can be represented as $a + b\alpha + c\alpha^2$, where $a, b, c \in \mathbb{F}_5$.

(c) Find $(1+\alpha)^{-1}$ (that is, find the coefficients in its expression as $a + b\alpha + c\alpha^2$).

4. Let $R = \mathbb{Q}[x]/((x-1)^3(x-2))$.

(a) Describe all the nilpotent elements in R. (Recall that an element a is called *nilpotent* if it satisfies $a^m = 0$ for some m).

(b) Describe all maximal ideals of R.

(c) Prove that in this ring the set of nilpotent elements coincides with the intersection of all the maximal ideals.

5. (a) Describe the quotient ring $\mathbb{R}[x]/((x^2-2x+1)(x+1)(x^2-9))$ in as simple terms as possible (that is, find a simpler-looking ring isomorphic to it).

(b) Prove that there exists a polynomial $f \in \mathbb{R}[x]$ such that: $f(1) = 1$ and $f'(1) = 0$, $f(-1) = 2$, $f(3) = f(-3) = 3$.

6. Let N be the submodule of $\mathbb{Z}^3$ generated by the vectors $\langle 2,0,3\rangle$, $\langle 2,2,0\rangle$, and $\langle 4,2,3\rangle$.

(a) Is N free? If yes, find the rank of N.

(b) Find the quotient $\mathbb{Z}^3/N$.

7. Let R be a ring with 1 (not necessarily commutative), and let M be a left R-module.

(a) An element $e \in R$ is called an *idempotent* if $e^2 = e$ and e is a central element of R. If e is an idempotent, prove that $M = eM \oplus (1-e)M$.

(b) Let $A \in M_n(\mathbb{R})$ be an $n \times n$-matrix. Then A defines a linear operator from $\mathbb{R}^n$ to itself; denote this linear operator by P. Prove that if $A^2 = A$, then $\mathbb{R}^n = \mathrm{Ker}(P) \oplus \mathrm{Im}(P)$ (as a direct sum of $\mathbb{R}$-vector spaces), where $\mathrm{Ker}(P) = \{v \in \mathbb{R}^n \mid Pv = 0\}$, and $\operatorname{Im} P$ is the image of $\mathbb{R}^n$ under P (you can assume that kernel and image are vector subspaces, no need to prove it).