University of Ottawa

Department of Mathematics and Statistics

MAT 3143: Ring Theory

Professor: Hadi Salmasian

Final Exam

April 18, 2011

Surname _____ First Name _____

Student # _____

Instructions:

(a) You have three hours to complete this exam.
(b) The number of points available for each question is indicated in square brackets.
(c) All work to be considered for grading should be written in the space provided. The reverse side of pages is for scrap work. If you find that you need extra space in order to answer a particular question, you should continue on the reverse side of the page and indicate this **clearly**. Otherwise, the work written on the reverse side of pages will not be considered for marks.
(d) Write your student number at the top of each page in the space provided.
(e) No notes, books, scrap paper, calculators or other electronic devices are allowed.
(f) You are strongly recommended to write in **pen**, not pencil.
(g) You may use the last page of the exam as scrap paper.

Good luck!

Please do not write in the table below.

Question	1	2	3	4	5	6	7	8	9	10	11	12	Total
Maximum	4	4	4	5	4	4	4	5	6	4	4	2	50
Grade													

1. **[4 pts]** Factor the polynomial $f(x) = 2x^4 + x + 2$ into a product of irreducible polynomials in $\mathbb{Z}_5[x]$.

Solution: The first thing to examine is whether or not $f(x)$ has a root in $\mathbb{Z}_5$. By a simple calculation one sees that $x = 1$ is a root and therefore $f(x) = (x-1)g(x)$. By a long division in $\mathbb{Z}_5[x]$ we have:

$$
\begin{array}{r|l}
x-1 & 2x^3+2x^2+2x+3 \\
\hline
 & 2x^4 \qquad\qquad +x \quad +2 \\
- & 2x^4 \quad -2x^3 \\
\cline{2-2}
 & \quad 2x^3 \\
 & - \quad 2x^3 \quad -2x^2 \\
\cline{2-2}
 & \qquad\quad 2x^2 \quad +x \\
 & - \qquad 2x^2 \quad -2x \\
\cline{2-2}
 & \qquad\qquad\quad 3x \quad +2 \\
 & \qquad - \qquad 3x \quad -3 \\
\cline{2-2}
 & \qquad\qquad\quad 0x \quad +5 \quad = 0
\end{array}
$$

Therefore we have $2x^4 + x + 2 = (x-1)(2x^3 + 2x^2 + 2x + 3)$.

The polynomial $2x^3 + 2x^2 + 2x + 3$ has degree at most three, and by a theorem proved in class it is irreducible if and only if it does not have a root. It is easy to check directly that this polynomial does not have a root in $\mathbb{Z}_5$ and therefore it should be irreducible in $\mathbb{Z}_5[x]$.

2. **[4 pts]** Prove that the polynomial $q(x) = 3x^3 + 5x - 1$ is irreducible in $\mathbb{Q}[x]$.

Solution: Since the degree of the polynomial is at most 3, by a theorem proved in class it is irreducible if and only if it does not have any roots in $\mathbb{Q}$. By the Rational Roots Theorem we know that the roots of $q(x)$ should be among $\{1, -1, \frac{1}{3}, -\frac{1}{3}\}$. However, by direct calculation one can see that none of these numbers is a root of $q(x)$. Therefore $q(x)$ is irreducible.

3. **[4 pts]** Let $\mathbb{F}$ be a field. Find all of the idempotent elements of the ring $R = \mathbb{F}[x]/A$, where A is the ideal generated by x^2, i.e., $A = \langle x^2 \rangle$.

Solution: Elements of R are representable in a unique way in the form $a + b\overline{x}$ where $a, b \in \mathbb{F}$. (Here $\overline{x} = A + x$.) Now let $r = a + b\overline{x}$ be idempotent, i.e., $r^2 = r$. Then

$$(a + b\overline{x})^2 = a^2 + 2ab\overline{x}$$

and therefore we have $a = a^2$, $2ab = b$. Since $\mathbb{F}$ is a field, $a^2 = a$ implies that $a = 0, 1$. Therefore we obtain $b = 0$, i.e., the only idempotents of R are 0 and 1.

4.

(a) **[2 pts]** Write the statement of the Chinese Remainder Theorem for any ring R.

Solution: Let A and B be ideals of R. If $A + B = R$ then:

$$R/A \cap B \simeq R/A \times R/B.$$

(b) **[2 pts]** How many units does $\mathbb{Z}_{65}$ have? You should justify your answer.

Solution: Since $65 = 13 \times 5$, by the Chinese Remainder Theorem we have $\mathbb{Z}_{65}^* \simeq \mathbb{Z}_5^* \times \mathbb{Z}_{13}^*$. Therefore $\mathbb{Z}_{65}$ has $4 \times 12 = 48$ units.

(c) **[1 pts]** How many ideals does $\mathbb{Z}_{65}$ have? You should justify your answer.

Solution: If R and S are two rings then any ideal of $R \times S$ is of the form $A \times B$ where A is an ideal of R and B is an ideal of S. But $\mathbb{Z}_{13}$ and $\mathbb{Z}_5$ are fields, and therefore each of them has two ideals. Therefore $\mathbb{Z}_{65}$ has four ideals.

5.

(a) **[2 pts]** Write the definition of a Euclidean domain.

Solution: An integral domain R is called a Euclidean domain iff there exists a mapping

$$\delta : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

such that :

E1. Given $a, b \in R$ such that $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$.

E2. If $a \neq 0$ and $b \neq 0$ in R then $\delta(ab) \geq \delta(a)$.

(b) **[2 pts]** Prove the following theorem : every Euclidean domain is a PID.
(Recall that PID means principal ideal domain.)

Solution: Let R be a Euclidean domain and $A \neq \{0\}$ an ideal of R. Consider a nonzero element $a \in A$ such that $\delta(a)$ is smallest possible. Clearly $\langle a \rangle \subseteq A$. We now show that $A \subseteq \langle a \rangle$:

Let $b \in A$. Using (E1) we can find $r, q \in R$ such that $b = qa + r$ and $r = 0$ or $\delta(r) < \delta(a)$. But note that $r = b - qa \in A$ and therefore if $r \neq 0$ then by the choice of a we should have $\delta(r) \geq \delta(a)$, which is a contradiction. It follows that $r = 0$, hence $b \in \langle a \rangle$.

6.

(a) **[2 pts]** Let $\mathbb{F} \subseteq \mathbb{E}$ be a field extension and $u \in \mathbb{E}$ be algebraic over $\mathbb{F}$. Write the definition of the minimal polynomial of u over $\mathbb{F}$.

Solution: A nonconstant polynomial $m(x) \in \mathbb{F}[x]$ is a minimal polynomial of u over $\mathbb{F}$ iff (i) $m(u) = 0$, (ii) $m(x)$ is monic, and (iii) degree of $m(x)$ is smallest possible.

(b) **[2 pts]** Prove the following Theorem :

Let $\mathbb{F} \subseteq \mathbb{E}$ be a finite extension and $[\mathbb{E} : \mathbb{F}] = n$. If $u \in \mathbb{E}$ then there exists a nonzero polynomial $f(x) \in \mathbb{F}[x]$ such that $f(u) = 0$ and $\deg(f(x)) \leq n$.

Solution: Since $\dim_{\mathbb{F}} \mathbb{E} = n$, the $n + 1$ elements $1, u, \ldots, u^n$ are linearly independent over $\mathbb{F}$. It follows that there exist $a_0, \ldots, a_n \in \mathbb{F}$, non all zero, such that $a_0 + a_1 u + \cdots + a_n u^n = 0$. The statement of the theorem is satisfied by the polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$.

7.

(a) **[2 pts]** Let $u = \sqrt{3+\sqrt{12}}$. Find the minimal polynomial of u over $\mathbb{Q}$. You should justify your answer.

Solution: We have :

$$x = \sqrt{3+\sqrt{12}} \Rightarrow x^2 = 3+\sqrt{12} \Rightarrow (x^2-3)^2 = 12 \Rightarrow x^4 - 6x^2 - 3 = 0.$$

This polynomial is irreducible (Eisenstein criterion for $p = 3$) and u is its root. Therefore this polynomial is the minimal polynomial of u.

(b) **[2 pts]** Let $v = \sqrt{3-\sqrt{12}}$. Explain why $\mathbb{Q}(u) \simeq \mathbb{Q}(v)$. Is it also true that $\mathbb{Q}(u) = \mathbb{Q}(v)$? Justify your answer.

Solution: An argument similar to the previous part shows that the minimal polynomial of $\sqrt{3-\sqrt{12}}$ over $\mathbb{Q}$ is also x^4-6x^2-3. Therefore by a theorem about simple extensions we know that both of the extensions are equal to the quotient ring

$$\mathbb{Q}[x]/\langle x^4 - 6x^2 - 3\rangle.$$

This proves that $\mathbb{Q}(u) \simeq \mathbb{Q}(v)$.

However, $u \in \mathbb{R}$ and therefore the field

$$\mathbb{Q}(u) = \{\ a_0 + a_1u + a_2u^2 + a_3u^3\ :\ a_0, a_1, a_2, a_3 \in \mathbb{Q}\ \}$$

is a subfield of $\mathbb{R}$, whereas $v \notin \mathbb{R}$ because $3 - \sqrt{12} < 0$.

8. **[5 pts]** Find a splitting field $\mathbb{Q} \subseteq \mathbb{E}$ for $f(x) = (x^2 - 3)(x^2 + x + 1)$, and compute $[\mathbb{E} : \mathbb{Q}]$. You should justify your answers.

Solution: Let $i = \sqrt{-1}$. Clearly we have $\mathbb{E} = \mathbb{Q}(\sqrt{3}, -\sqrt{3}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}) = \mathbb{Q}(\sqrt{3}, \sqrt{-3})$. We now show that $[\mathbb{E} : \mathbb{Q}] = 4$. First observe that:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{E}.$$

The minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is $x^2 - 3$, and therefore

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \deg(x^2 - 3) = 2.$$

We have $\mathbb{E} \neq \mathbb{Q}(\sqrt{3})$ because $\sqrt{-3} \notin \mathbb{R}$ whereas $\mathbb{Q}(\sqrt{3}) = \{\, a_0 + a_1\sqrt{3} \;:\; a_0, a_1 \in \mathbb{Q} \,\} \subseteq \mathbb{R}$ and therefore $[\mathbb{E} : \mathbb{Q}(\sqrt{3})] \geq 2$. At the same time, we have

$$[\mathbb{E} : \mathbb{Q}(\sqrt{3})] \leq \deg(x^2 + 3) = 2$$

which proves that $[\mathbb{E} : \mathbb{Q}(\sqrt{3})] = 2$. By the Multiplication Theorem, it follows that $[\mathbb{E}, \mathbb{Q}] = 4$.

9. Let $i = \sqrt{-1}$ and consider the ring

$$\mathbb{Z}[\,i\,] = \{\ a + bi\ :\ a, b \in \mathbb{Z}\ \}$$

of Gaussian integers.

(a) **[4 pts]** Prove that $1 + 2i$ is a prime element of $\mathbb{Z}[\,i\,]$.

Solution: Since $\mathbb{Z}[\,i\,]$ is a UFD, every irreducible is prime. To show $1 + 2i$ is irreducible, we use $N(x + yi) = x^2 + y^2$. Note that:

$$N(x + yi) = 1 \Rightarrow x^2 + y^2 = 1 \Rightarrow \left\{ \begin{array}{l} x = 0 \\ y = \pm 1 \end{array} \right. \text{ or } \left\{ \begin{array}{l} x = \pm 1 \\ y = 0 \end{array} \right. \Rightarrow x + iy \text{ is a unit.}$$

Now

$$1 + 2i = r_1 r_2 \Rightarrow 5 = N(1 + 2i) = N(r_1)N(r_2) \Rightarrow N(r_1) = 1 \text{ or } N(r_2) = 1$$

which proves that $1 + 2i$ is irreducible.

(b) **[2 pts]** Let $r \in \mathbb{Z}[\,i\,]$ be a prime element. Prove that $\overline{r}$ is also a prime element of $\mathbb{Z}[\,i\,]$. (Here $\overline{r}$ means the complex conjugate of r.)

Solution: Suppose $\overline{r} | r_1 r_2$ where $r_1, r_2 \in \mathbb{Z}[\,i\,]$. Then:

$$r_1 r_2 = \overline{r}s \Rightarrow \overline{r}_1 \overline{r}_2 = r\overline{s} \Rightarrow r | \overline{r}_1 \overline{r}_2 \Rightarrow r | \overline{r}_1 \text{ or } r | \overline{r}_2 \Rightarrow \overline{r} | r_1 \text{ or } \overline{r} | r_2.$$

10. Let p be a prime number.

(a) **[2 pts]** Are $GF(p^2)$ and $\mathbb{Z}_p \times \mathbb{Z}_p$ isomorphic? You should justify your answer, i.e., either prove or disprove this statement.

Solution: No, because $\mathbb{Z}_p \times \mathbb{Z}_p$ is not a field: for example the element $(1, 0)$ is nonzero but not a unit.

(b) **[2 pts]** How many subfields does $GF(p^8)$ have? You should justify your answer.

Solution: By a theorem, we know that for any positive integer m, there exists a unique subfield of $GF(p^8)$ with p^m elements if and only if $m|8$. The divisors of 8 are $1, 2, 4, 8$ and therefore $GF(p^8)$ has four subfields.

11. Let $\mathbb{O} = \{\ldots, -3, -1, 1, 3, \ldots\}$ be the set of odd integers and $\mathbb{P} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ be the set of even integers. Consider the ring

$$R = \{\ \frac{m}{n}\ :\ m \in \mathbb{Z} \text{ and } n \in \mathbb{O}\ \}$$

with the usual addition and multiplication of rational numbers.

(a) **[1 pt]** Find all of the units of R.

Solution: The inverse of $\frac{m}{n}$ is $\frac{n}{m}$, and it belongs to R if and only if both m and n are odd. Therefore the units of R are elements of form $\frac{m}{n}$ where both m and n are odd.

(b) **[2 pts]** Prove that the set

$$A = \{\ \frac{m}{n}\ :\ m \in \mathbb{P} \text{ and } n \in \mathbb{O}\ \}$$

is a maximal ideal of R.

Solution: To show that A is an ideal note that:

$$\frac{2m}{n} \in A \text{ and } \frac{2m'}{n'} \in A \Rightarrow \frac{2m}{n} \pm \frac{2m'}{n'} = \frac{2mn' \pm 2m'n}{nn'} \in A$$

and

$$\frac{r}{s} \in R \text{ and } \frac{2m}{n} \in A \Rightarrow \frac{r}{s}\frac{2m}{n} = \frac{2rm}{sn} \in A.$$

To show that A is in fact maximal, note that any element $r \in R \setminus A$ is a unit, and therefore if B is an ideal such that $A \subsetneq B$, then B should contain units, i.e., $B = R$.

(c) **[1 pt]** Does R have any maximal ideals other than A? Justify your answer.

Solution: No, because every element of $R \setminus A$ is a unit, and therefore if B is any ideal of R such that $B \neq R$ then $B \cap R \setminus A = \varnothing$, i.e., $B \subseteq A$.

12. **[2 pts]** Prove that for every positive integer n, the polynomial $x^n - \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2})$.

Solution: By a theorem (stating the index of a simple extensions is equal to the degree of the minimal polynomial) it is enough to show that $[\mathbb{Q}(\sqrt[2n]{2}) : \mathbb{Q}(\sqrt{2})] = n$. But note that

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[2n]{2})$$

and we have:

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2 - 2) = 2$ because $x^2 - 2$ is irreducible over $\mathbb{Q}$ (Eisenstein for $p = 2$).

$[\mathbb{Q}(\sqrt[2n]{2}) : \mathbb{Q}] = \deg(x^{2n} - 2) = 2n$ because $x^{2n} - 2$ is irreducible over $\mathbb{Q}$ (Eisenstein for $p = 2$).

The claim $[\mathbb{Q}(\sqrt[2n]{2}) : \mathbb{Q}(\sqrt{2})] = n$ now follows by an application of the Multiplication Theorem.