University of Ottawa

Department of Mathematics and Statistics

MAT3143: Ring Theory
Professor: Hadi Salmasian

Final Exam

April 21, 2015

Surname ____________________ First Name ____________________

Student # ____________________

Instructions:

(a) You have 3 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	6	5	5	10	6	4	5	3	5	4	7	4	64
Grade													

1. (a) [**3 points**] Write the definition of a Euclidean domain.

   (b) [**3 points**] Prove that every Euclidean domain is a PID.

2. Let $\mathbb{F} \subseteq \mathbb{K}$ be a field extension.

(a) [**2 points**] Write down the definition of the minimal polynomial of an element $u \in \mathbb{K}$ over $\mathbb{F}$.

(b) [**3 points**] Let $u \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Let $f(x) \in \mathbb{F}[x]$ be a polynomial such that $f(u) = 0$. Let $m(x)$ be the minimal polynomial of u over $\mathbb{F}$. Prove that $m(x)|f(x)$.

3. For each of the following statements, write **T** if it is true, and write **F** if it is false. You do not need to justify your answer.

For each incorrect answer you will lose 1 point. (You will not lose any points if you leave the answer area blank.)

(a) [**1 point**] An ideal $I \subseteq R$ of a ring R is maximal if and only if the quotient ring R/I is a field.

(b) [**1 point**] Every prime element of the ring

$$R = \mathbb{Z}[\sqrt{2}, \sqrt{3}] = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \ : \ a, b, c, d \in \mathbb{Z}\right\}$$

is irreducible.

(c) [**1 point**] For every integer $n \geq 2$, the polynomial $f(x) = x^{2n} + 4x^3 + 2nx + 4n^2 + 2$ is irreducible in $\mathbb{Q}[x]$.

(d) [**1 point**] Every polynomial of odd degree with coefficients in $\mathbb{R}$ decomposes as a product of linear factors.

(e) [**1 point**] In any ring R, an element $a \in R$ is idempotent if and only if $1 - a \in R$ is idempotent.

4. For each of the following parts, provide an example. You should justify that your example satisfies the given requirements.

(a) [**2 points**] An idempotent element of $R = M_2(\mathbb{Z})$ other than $0, 1 \in R$.

(b) [**2 points**] A proper subring of $\mathbb{Q}$ other than $\mathbb{Z}$.

(c) [**2 points**] A polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(x)$ is not an irreducible element of the ring $\mathbb{Z}[x]$ but it is an irreducible element of the ring $\mathbb{Q}[x]$.

(continued from last page)

(d) [**2 points**] A real number $\alpha \in \mathbb{R}$ which is transcendental over the field $\mathbb{Q}(\sqrt[3]{2})$.

(e) [**2 points**] A monic cubic polynomial $f(x) \in \mathbb{Z}[x]$ whose reduction mod p is reducible in $\mathbb{Z}_p[x]$ for $p = 2, 3, 5$, and irreducible for $p = 7$.

5. (a) [**3 points**] Write down the definition of greatest common divisor (gcd) in an integral domain.

(b) [**3 points**] Let R be a PID and $a, b \in R$ such that $ab \neq 0$. Set $A = \langle a \rangle$ and $B = \langle b \rangle$, so that A and B are the principal ideals generated by a and b. Define $A + B = \{x + y \ : \ x \in A \text{ and } y \in B\}$. Prove that $A + B$ is equal to the principal ideal generated by $\gcd(a, b)$.

6. [**4 points**] Let $\mathbb{F} \subseteq \mathbb{K}$ be a finite extension of fields (i.e., $[\mathbb{K} : \mathbb{F}] < \infty$]). Set $m = [\mathbb{K} : \mathbb{F}]$, and let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree $n > 1$, such that $\gcd(m, n) = 1$. Suppose that $f(u) = 0$ for some $u \in \mathbb{K}$. Prove that $f(x)$ is reducible in $\mathbb{F}[x]$.

7. Let p be a prime number and $n \geq 1$. Set $\mathbb{F}_{p^n} = \mathrm{GF}(p^n)$.

(a) **[2 points]** Prove that the Frobenius homomorphism

$$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \ , \ a \mapsto a^p$$

is an automorphism of the field $\mathbb{F}_{p^n}$.

(b) **[3 points]** Prove that for every $\alpha \in \mathbb{F}_{p^n}$, the polynomial $x^p - \alpha$ decomposes in $\mathbb{F}_{p^n}[x]$ into a product of linear factors. Determine the root multiplicities of $x^p - \alpha$.

8. [**3 points**] Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$ be an irreducible polynomial, and n be a positive integer. Let I denote the principal ideal of $\mathbb{F}[x]$ that is generated by

$$f(x)^n = \underbrace{f(x) \cdots f(x)}_{n \text{ times}}.$$

Determine the nilpotent elements of the quotient ring $\mathbb{F}[x]/I$ explicitly. You should justify your answer.

9. (a) [**2 points**] Write the definition of the ACCP condition.

(b) [**3 points**] Prove that $\mathbb{Z}[x]$ satisfies the ACCP condition.

10. [**4 points**] Let $\mathbb{Q} \subseteq \mathbb{E}$ be a finite extension of fields (i.e., $[\mathbb{E} : \mathbb{Q}] < \infty$). Prove that for every ring homomorphism $\sigma : \mathbb{Z}[x] \to \mathbb{E}$ we have $\ker(\sigma) \neq \{0\}$.

11. [**7 points**] Let $\mathbb{E}$ be the splitting field of $f(x) = (x^2+2)(x^3+1)$ over $\mathbb{Q}$. Find a basis of $\mathbb{E}$ over $\mathbb{Q}$. You should describe your basis explicitly. You should justify your answer.

12. [**4 points**] Determine all of the maximal ideals of $\mathbb{Z}_{70}$. You should justify your answer.

This page is intentionally left blank. You may use it as scrap paper.