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.

Solution: Let R be an integral domain. We call R a *Euclidean domain* if there exists a map

$$\delta : R \setminus \{0\} \to \mathbb{N}_0 = \{0, 1, 2, \ldots\}$$

which verifies the following conditions:

(E1) For every $a \in R$ and every $b \in R$ such that $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and

$$\text{either } r = 0 \text{ or } \delta(r) < \delta(b)$$

(E2) $\delta(ab) \geq \delta(a)$ for every non-zero elements $a, b \in R$.

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

Solution: Let R be a Euclidean domain, and let $I \subseteq R$ be a non-zero ideal of R. We choose $b \in I \setminus \{0\}$ such that $\delta(b)$ is the smallest possible. We will now show that $I = \langle b \rangle$:

$$\begin{aligned} a \in I \text{ and } a \notin \langle b \rangle &\Rightarrow a = bq + r \text{ and } r \neq 0 \\ &\Rightarrow r = a - bq \in I \text{ and } \delta(r) < \delta(b) \text{ contradiction.} \end{aligned}$$

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 $\mathbb{F}$.

Solution: The *minimal polynomial* of u over $\mathbb{F}$ is the unique monic polynomial $m(x) \in \mathbb{F}[x]$ of smallest degree which satisfies $m(u) = 0$.

(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 $m(x)|f(x)$.

Solution: We set $d(x) := \gcd(f(x), m(x))$. There exist polynomials $a(x), b(x) \in \mathbb{F}[x]$ such that

$$d(x) = a(x)f(x) + b(x)m(x).$$

Then $d(u) = a(u)f(u) + b(u)m(u) = 0$, and consequently, $d(x) \neq 1$. Now write $m(x) = d(x)g(x)$. Since $m(x)$ is irreducible, this factorization should be trivial, that is, $g(x) \in \mathbb{F}^*$. Since both $d(x)$ and $m(x)$ are monic, it follows that $d(x) = m(x)$, and therefore $m(x)|f(x)$.

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.

Solution: False. R/I is simple but not necessarily 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.

Solution: True. R is an integral domain, and every prime element of an integral domain 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 $\mathbb{Q}[x]$.

Solution: True. Follows from Eisenstein for $p = 2$.

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

Solution: False.

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

Solution: True. $a^2 = a \Rightarrow (1-a)^2 = 1 - 2a + a^2 = 1 - 2a + a = 1 - a$.

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 $0, 1 \in R$.

Solution: For example, $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$

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

Solution: For example, $\mathbb{Z}[\frac{1}{2}] = \left\{ \frac{m}{2^n} \ : \ m, n \in \mathbb{Z} \right\}$.

(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 $\mathbb{Q}[x]$.

Solution: $f(x) = 2(x^2 + 1)$ is not irreducible in $\mathbb{Z}[x]$ (because $2 \in \mathbb{Z}[x]$ is not a unit).

(continued from last page)

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

Solution: $\alpha = \pi = 3.14\cdots$ because if α is algebraic over $\mathbb{Q}(\sqrt[3]{2})$, then α is also algebraic over $\mathbb{Q}$, which contradicts Lindemann's Theorem.

(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 $p = 7$.

Solution: Note that $x^3 = \pm 1$ in $\mathbb{Z}_7$, so that $f(x) = x^3 + 2$ does not have any roots in $\mathbb{Z}_7$. But it is easy to check that the latter polynomial has roots in $\mathbb{Z}_p$ for $p = 2, 3, 5$.

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

Solution: Let R be an integral domain and $a_1, \ldots, a_n \in R$ be on-zero elements. An element $d \in R$ is called the *gcd* of $a_1, \ldots, a_n$ if it verifies the following conditions:

- $d|a_1, \ldots, d|a_n$.
- $\forall_{r \in R} : r|a_1, \ldots, r|a_n \Rightarrow r|d$.

(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 $\gcd(a, b)$.

Solution: Set $d = \gcd(a, b)$. For every $x \in A$ and $y \in B$ we have $d|x$ and $d|y$, so that $d|x + y$. Thus $A + B \subseteq \langle d \rangle$. To complete the proof, it is enough to show that $d \in A + B$. This follows from Theorem 2.82, which implies that $d = ax_1 + by_1$ for some $x_1, y_1 \in R$.

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 $\mathbb{F}[x]$.

Solution: Suppose that $f(x)$ is irreducible. Then $[\mathbb{F}(u) : \mathbb{F}] = \deg(f(x)) = n$. On the other hand, the Multiplication Theorem implies that $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}(u)][\mathbb{F}(u) : \mathbb{F}]$, so that $n|m$, which is a contradiction because $\gcd(m, n) = 1$.

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 $\mathbb{F}_{p^n}$.

Solution: The Frobenius homomorphism is a ring homomorphism. Since $\mathbb{F}_{p^n}$ is a field, the kernel of the Frobenius homomorphism, which is an ideal of $\mathbb{F}_{p^n}$, should be the zero ideal. Thus the Frobenius homomorphism is injective. Since $\mathbb{F}_{p^n}$ is finite, every injection $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is also a surjection.

(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 $x^p - \alpha$.

Solution: By (a) we can write $\alpha = \beta^p$ for some $\beta \in \mathbb{F}_{p^n}$. Therefore

$$x^p - \alpha = x^p - \beta^p = (x - \beta)^p.$$

Therefore the polynomial $x^p - \alpha$ has only one root with multiplicity p.

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.

Solution: Suppose that $I+g(x)$ is a nilpotent element of $\mathbb{F}[x]/I$. Then $\big(I+g(x)\big)^m = I+g(x)^m$ and from nilpotence of $I + g(x)$ it follows that $g(x)^m \in I$, so that $f(x)^n | g(x)^m$. Since $f(x)$ is irreducible, we obtain $f(x)|g(x)$. Conversely, for any polynomial $g(x)$ which satisfies $f(x)|g(x)$, we obtain $\big(I + g(x)\big)^n = I$.

In conclusion, an element $I + g(x)$ is nilpotent if and only if $f(x)|g(x)$.

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

Solution: We say that an integral domain R satisfies the condition $ACCP$ if every increasing sequence of principal ideals of R stabilizes. In otherwords, for for every sequence of ideals

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$$

there exists an $n \in \mathbb{Z}^+$ such that $\langle a_n \rangle = \langle a_{n+1} \rangle = \cdots$.

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

Solution: Since $\mathbb{Z}$ is a UFD, the ring $\mathbb{Z}[x]$ is also a UFD (Theorem 2.76). Every UFD satisfies the ACCP condition (Theorem 2.71).

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 $\ker(\sigma) \neq \{0\}$.

Solution: Set $u = \sigma(x)$. If $u = 0$ then $x \in \ker(\sigma)$ and we are done. Assume that $u \neq 0$. Since $u \in \mathbb{E}$ is algebraic over $\mathbb{Q}$, there exists a non-constant polynomial $f(\mathsf{x}) = a_0 + a_1\mathsf{x} \cdots + a_n\mathsf{x}^n \in \mathbb{Q}[\mathsf{x}]$ such that $f(u) = 0$. After multiplying $f(\mathsf{x})$ by a sufficiently large integer, we can assume that indeed $f(\mathsf{x}) \in \mathbb{Z}[\mathsf{x}]$. Then

$$\sigma(a_0 + a_1x + \cdots + a_nx^n) = f(u) = 0,$$

that is, $a_0 + a_1x + \cdots + a_nx^n \in \ker(\sigma)$.

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.

Solution: We have $x^3+1 = (x+1)(x^2-x+1)$. Now let $\omega \in \mathbb{C}$ denote a root of the polynomial $x^2 - x + 1$. The other root of this polynomial is $1 - \omega$ (because the sum of roots is equal to 1). Therefore we have the extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\sqrt{-2}, \omega)$$

and the polynomial $f(x)$ splits in $\mathbb{Q}(\sqrt{-2}, \omega)$ as

$$(x - \sqrt{-2})(x + \sqrt{-2})(x + 1)(x - \omega)(x - (1 - \omega)).$$

Since $\mathbb{E} = \mathbb{Q}(\sqrt{-2}, \omega)$ is generated over $\mathbb{Q}$ by the roots of $f(x)$, it is the splitting field of $f(x)$. We now prove that $[\mathbb{Q}(\sqrt{-2}, \omega) : \mathbb{Q}] = 4$. By Eisenstein for $p = 2$, the polynomial $x^2 + 2$ is irreducible in $\mathbb{Q}[x]$, and therefore $[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2$, with basis $\{1, \sqrt{-2}\}$. Next note that

$$[\mathbb{Q}(\sqrt{-2}, \omega) : \mathbb{Q}(\sqrt{-2})] = [\mathbb{Q}(\sqrt{-2})(\omega) : \mathbb{Q}(\sqrt{-2})] \leq \deg(x^2 - x + 1) = 2.$$

Finally we show that equality holds in the latter inequality. To this end, it is enough to prove that $\mathbb{Q}(\sqrt{-2}, \omega) \neq \mathbb{Q}(\sqrt{-2})$. Assume, on the contrary, that $\mathbb{Q}(\sqrt{-2}, \omega) = \mathbb{Q}(\sqrt{-2})$, so that $\omega \in \mathbb{Q}(\sqrt{-2})$. This means that

$$\omega = a + b\sqrt{-2} \text{ for } a, b \in \mathbb{Q}.$$

it follows that

$$\omega - 1 = \omega^2 = (a + b\sqrt{-2})^2 = a^2 - 2b^2 + 2ab\sqrt{-2}$$

from which it follows that

$$(a - 1) + b\sqrt{-2} = (a^2 - 2b^2) + 2ab\sqrt{-2}.$$

Thus we obtain

$$\begin{cases} a - 1 = a^2 - 2b^2 \\ b = 2ab. \end{cases}$$

Now if $b = 0$ then $\omega = a \in \mathbb{Q}$ which is a contradiction because $x^2 - x + 1$ has no roots in $\mathbb{Q}$. If $b \neq 0$, then $2a = 1$ and thus $a = \frac{1}{2}$, hence $\frac{1}{4} - 2b^2 = -\frac{1}{2}$, that is, $b^2 = \frac{3}{8}$, which is a contradiction because it implies that $b = \sqrt{\frac{3}{8}} \notin \mathbb{Q}$. This completes the proof of the claim that $\mathbb{Q}(\sqrt{-2}, \omega) \neq \mathbb{Q}(\sqrt{-2})$.

From the Multiplication Theorem we now obtain the basis

$$\{1, \sqrt{-2}, \omega, \sqrt{-2}\omega\}.$$

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

Solution: The ideals of $\mathbb{Z}_{70}$ are in bijective correspondence with ideals of $\mathbb{Z}$ which contain $70\mathbb{Z} = \{70k \ : \ k \in \mathbb{Z}\}$. Moreover, $\mathbb{Z}$ is a PID and $70\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m|70$. Maximal ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$ for a prime number p. Since $70 = 2 \times 5 \times 7$, the maximal ideals of $\mathbb{Z}_{70}$ are $2\mathbb{Z}_{70}$, $5\mathbb{Z}_{70}$, and $7\mathbb{Z}_{70}$.