University of Ottawa
Department of Mathematics and Statistics

MAT 3143: Ring Theory
Professor: Alistair Savage

Final Exam – Solutions
April 2013

Surname _____ First Name _____

Student # _____

Instructions:

(a) You have 3 hours to complete this exam.
(b) This exam consists of two parts. Questions 1 through 5 are **answer only**. For these questions, only your final answer will be considered for marks. Questions 6 through 13 are **long answer**. For these questions, you must show your work and justify your answers to receive full marks. Partial marks may be awarded for making sufficient progress towards a solution.
(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 may use the last page of the exam as scrap paper.

Good luck!

Please do not write in the table below.

Question	1–5	6	7	8	9	10	11	12	13	Total
Maximum	12	3	3	8	6	4	4	5	3	48
Grade										

Part A: Answer Only Questions

For Questions 1–5, only your final answer will be considered for marks. Write your final answers in the spaces provided.

1. **(2 pts)** Consider the following classes of rings:
   (a) integral domains
   (b) fields
   (c) euclidean domains
   (d) commutative rings
   (e) UFDs
   (f) PIDs

Organize these classes (using the letters (a)–(f)) into a chain of class inclusions.

Answer:

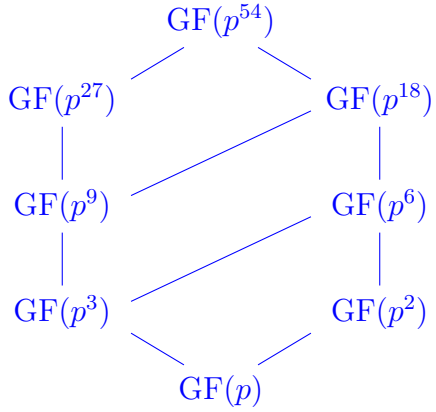
$$\text{(b)} \subseteq \text{(c)} \subseteq \text{(f)} \subseteq \text{(e)} \subseteq \text{(a)} \subseteq \text{(d)}$$

2. **(2 pts)** Which of the following statements is/are true?
   (a) All finite field extensions are algebraic.
   (b) All algebraic field extensions are finite.
   (c) In any integral domain, all irreducible elements are prime.
   (d) In any integral domain, all prime elements are irreducible.
   (e) In any commutative ring, all maximal ideals are prime ideals.
   (f) In any commutative ring, all prime ideals are maximal ideals.

Answer: (a), (d), (e)

3. **(2 pts)** Draw the lattice of subfields of $\mathrm{GP}(p^{54})$, where p is a prime number.

Answer:



4. **(2 pts)** Which of the following statements is/are true?

(a) If R is a UFD, then so is $R[x]$.
(b) If R is a PID, then so is $R[x]$.
(c) Greatest common divisors exist in any UFD.
(d) A subset of a ring R is an ideal of R if and only if it is the kernel of some ring homomorphism with domain R.
(e) The ring $\mathbb{Z}(i)$ of gaussian integers is a euclidean domain.
(f) The ring $\mathbb{Z}[x]$ is a euclidean domain.

Answer: (a), (c), (d), (e)

5. **(4 pts)** Give examples of the following.

(a) An irreducible polynomial in $\mathbb{Q}[x]$ of degree n, where n is an arbitrary positive integer.

Answer: The polynomial $x^n - 2$ is irreducible by the Eisenstein Criterion with $p = 2$.

(b) An algebraically closed field that is not the field of complex numbers.

Answer: The field of algebraic numbers is one example.

(c) A transcendental element over some field.

Answer: The number π is transcendental over $\mathbb{Q}$.

(d) A field extension of $\mathbb{Q}$ of degree six.

Answer: Since the polynomial $x^6 - 2 \in \mathbb{Q}[x]$ is irreducible (see above), the ideal $\langle x^6 - 2 \rangle$ is maximal (we are using here that $\mathbb{Q}[x]$ is a PID) and so $\mathbb{Q}[x]/\langle x^6 - 2 \rangle$ is a field extension of $\mathbb{Q}$ of degree six.

Part B: Long Answer Questions

For Questions 6–13, you must show your work and justify your answers to receive full marks. Partial marks may be awarded for making sufficient progress towards a solution.

6. **(3 pts)** Find the minimal polynomial of $u = \sqrt{7+\sqrt{14}}$ over $\mathbb{Q}$.

Solution: We have

$$u^2 = 7 + \sqrt{14} \implies (u^2-7)^2 = 14 \implies u^4 - 14u^2 + 35 = 0.$$

So, if we set $f(x) = x^4 - 14x^2 + 35$, then $f(u) = 0$. By the Eisenstein Criterion with $p = 7$, we see that $f(x)$ is irreducible. Therefore, it is the minimal polynomial of u.

7. **(3 pts)** Suppose that $\varphi\colon \mathbb{F} \to R$ is a ring homomorphism, where $\mathbb{F}$ is a field and R is a ring. Show that φ is either injective or is the zero map.

Solution: We know that $\ker\varphi$ is an ideal of $\mathbb{F}$. Since the only ideals of $\mathbb{F}$ are the zero ideal and $\mathbb{F}$ itself, we see that φ is either injective (when $\ker\varphi = \{0\}$) or is the zero map (when $\ker\varphi = \mathbb{F}$). Note that since $\varphi(1_{\mathbb{F}}) = 1_R$, we have that R is the zero ring if φ is the zero map.

8. Consider the polynomial $f(x) = x^4 - 5$.

(a) **(2 pts)** Find the splitting field $\mathbb{E}$ of $f(x)$ over $\mathbb{Q}$.

(b) **(4 pts)** Give a basis for $\mathbb{E}$ over $\mathbb{Q}$. What is $[\mathbb{E} : \mathbb{Q}]$?

(c) **(2 pts)** Find the splitting field $\mathbb{K}$ of $f(x)$ over $\mathbb{R}$. What is $[\mathbb{K} : \mathbb{R}]$?

Solution: We have

$$f(x) = (x^2 - \sqrt{5})(x^2 + \sqrt{5}) = (x - \sqrt[4]{5})(x + \sqrt[4]{5})(x - i\sqrt[4]{5})(x + i\sqrt[4]{5}).$$

(a) The splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{E} = \mathbb{Q}(\sqrt[4]{5}, -\sqrt[4]{5}, i\sqrt[4]{5}, -i\sqrt[4]{5}) = \mathbb{Q}(\sqrt[4]{5}, i)$.

(b) Consider the chain of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{5}) \subseteq \mathbb{Q}(\sqrt[4]{5}, i).$$

Since $x^4 - 5$ is irreducible over $\mathbb{Q}$ (applying the Eisenstein Criterion with $p = 5$), it is the minimal polynomial of $\sqrt[4]{5}$ over $\mathbb{Q}$. Thus $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$.

Since i is a root of $x^2+1 \in \mathbb{Q}(\sqrt[4]{5})[x]$, we have $[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})] \leq 2$. Because $i \notin \mathbb{Q}(\sqrt[4]{5})$ (since $\mathbb{Q}(\sqrt[4]{5}) \subseteq \mathbb{R}$), we also have $[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})] \geq 2$. Therefore, $[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})] = 2$. By the multiplication theorem, the vectors

$$1, \sqrt[4]{5}, (\sqrt[4]{5})^2, (\sqrt[4]{5})^3, i, i\sqrt[4]{5}, i(\sqrt[4]{5})^2, i(\sqrt[4]{5})^3$$

form a basis of $\mathbb{E}$ over $\mathbb{Q}$. Thus $[\mathbb{E} : \mathbb{Q}] = 8$.

(c) The splitting field of $f(x)$ over $\mathbb{R}$ is $\mathbb{K} = \mathbb{R}(i\sqrt[4]{5}) = \mathbb{R}(i) = \mathbb{C}$. Therefore $[\mathbb{K} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2$.

9. Let $f(x) = x^3 + 2x^2 - 10 \in \mathbb{Q}[x]$.
   (a) **(2 pts)** Show that $\mathbb{Q}[x]/\langle f(x)\rangle$ is a field.
   (b) **(1 pt)** Give a basis for $\mathbb{Q}[x]/\langle f(x)\rangle$ over $\mathbb{Q}$.
   (c) **(3 pts)** Write a multiplication table for this basis. That is, write a table that expresses the product of any two elements in the basis as a linear combination of the basis elements.

Solution:

(a) Applying the Eisenstein Criterion with $p = 2$, we see that $f(x)$ is irreducible. Since $\mathbb{F}[x]$ is a PID, this implies that $\langle f(x)\rangle$ is a maximal ideal of $\mathbb{Q}[x]$. Therefore, the quotient $\mathbb{Q}[x]/\langle f(x)\rangle$ is a field.

(b) Since $\deg f(x) = 3$, a basis for $\mathbb{Q}[x]/\langle f(x)\rangle$ is given by $1, t, t^2$, where $t = x + \langle f(x)\rangle$ is the coset of x in $\mathbb{Q}[x]/\langle f(x)\rangle$.

(c) Multiplication in terms of the basis $1, t, t^2$ is determined by the equality $f(t) = 0$. Thus we have $t^3 = -2t^2 + 10$. This also gives

$$t^4 = t(t^3) = t(-2t^2 + 10) = -2t^3 + 10t = -2(-2t^2 + 10) + 10t = 4t^2 + 10t - 20.$$

So we have the following multiplication table:

$\times$	1	t	t^2
1	1	t	t^2
t	t	t^2	$-2t^2 + 10$
t^2	t^2	$-2t^2 + 10$	$4t^2 + 10t - 20$

10. **(4 pts)** Suppose that R is a UFD. Show that if $a, b, c \in R$ satisfy

$$\gcd(a, b) \sim 1 \sim \gcd(a, c),$$

then $\gcd(a, bc) \sim 1$.

Solution: Let $p_1, \ldots, p_r$ be the nonassociated primes dividing one of a, b, c. Then we can write

$$\begin{aligned} a &\sim p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \quad a_i \in \mathbb{N}, \\ b &\sim p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}, \quad b_i \in \mathbb{N}, \\ c &\sim p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}, \quad c_i \in \mathbb{N}, \\ bc &\sim p_1^{b_1+c_1} p_2^{b_2+c_2} \cdots p_r^{b_r+c_r}. \end{aligned}$$

Since $\gcd(a, b) \sim 1$, we have $\min(a_i, b_i) = 0$ for all $i = 1, \ldots, r$. Similarly, since $\gcd(a, c) \sim 1$, we have $\min(a_i, c_i) = 0$ for all $i = 1, \ldots, r$. Thus, for each $i = 1, \ldots, r$, either $a_i = 0$ or $b_i = c_i = 0$ (in which case $b_i + c_i = 0$). This implies that $\min(a_i, b_i + c_i) = 0$ for all $i = 1, \ldots, r$. Hence $\gcd(a, bc) \sim 1$.

Alternate Solution: We prove the result by contradiction. Suppose that $\gcd(a, bc)$ is not a unit. Then, since R is a UFD, there is some irreducible element p dividing $\gcd(a, bc)$. Thus $p \mid a$ and $p \mid bc$. Since p is irreducible, it is prime (because R is a UFD), thus $p \mid b$ or $p \mid c$. If $p \mid b$, then $p \mid \gcd(a, b)$, contradicting the fact that $\gcd(a, b) \sim 1$. Similarly, if $p \mid c$, then $p \mid \gcd(a, c)$, contradicting the fact that $\gcd(a, c) \sim 1$.

11. **(4 pts)** Factor $f(x) = x^4 + x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ completely as a product of irreducibles.

Solution: Since 1 is a root of $f(x)$, we know that $x-1 = x+2$ is a factor of $f(x)$. Using polynomial division, we find that

$$f(x) = (x+2)(x^3 + 2x^2 + 2).$$

Since 2 is a root of $x^3 + 2x^2 + 2$, we know that it has $x - 2 = x + 1$ as a factor. We again use polynomial division to obtain

$$f(x) = (x+2)(x+1)(x^2 + x + 2).$$

Now, one easily checks that $x^2 + x + 2$ has no roots in $\mathbb{Z}_3$. Since it is of degree two, this implies that it is irreducible. Thus, the above expression is a factorization into irreducibles.

12. **(5 pts)** Suppose that R is a ring and I_n is an ideal of R for each positive integer n. Furthermore, suppose that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$.

(a) Show that $\bigcup_{n=1}^{\infty} I_n$ (i.e. the union of all the I_n) is an ideal of R.

(b) Show that if R is a PID, then there exists a positive integer N such that $I_N = I_k$ for all $k \geq N$.

Solution:

(a) Let $I = \bigcup_{n=1}^{\infty} I_n$. Since $0 \in I_n$ for all $n \in \mathbb{N}$, we have $0 \in I$. Suppose $a, b \in I$. Then $a \in I_n$ for some $n \in \mathbb{N}$ and $b \in I_m$ for some $m \in \mathbb{N}$. Let $N = \max(n, m)$. Then $a, b \in I_N$. Since I_N is an ideal, we have $a - b \in I_N \subseteq I$. So I is an additive subgroup of R.

Now suppose $r \in R$ and $a \in I$. Then $a \in I_n$ for some $n \in \mathbb{N}$. Thus $ra, ar \in I_n \subseteq I$. Therefore, I is an ideal of R.

(b) If R is a PID, then $I = \langle a \rangle$ for some $a \in R$. Then $a \in I_N$ for some N. Thus $I_N = I$. This implies that $I_N = I_k$ for all $k \geq N$.

13. **(3 pts)** Suppose $\mathbb{F}$ is a finite (nonzero) field. Show that $\mathbb{F}$ is not algebraically closed. *Hint:* Construct an explicit polynomial in $\mathbb{F}[x]$ that has no roots in $\mathbb{F}$.

Solution: Let

$$f(x) = 1 + \prod_{a \in \mathbb{F}} (x - a) \in \mathbb{F}[x].$$

This is polynomial since the product is finite. We clearly have $f(a) = 1 \neq 0$ for all $a \in \mathbb{F}$. Thus $f(x)$ has no roots in $\mathbb{F}$. So $\mathbb{F}$ is not algebraically closed.