MATH 113 FINAL EXAM (4.10PM-6PM)

PROFESSOR PAULIN

DO NOT TURN OVER UNTIL INSTRUCTED TO DO SO.
CALCULATORS ARE NOT PERMITTED
REMEMBER THIS EXAM IS GRADED BY A HUMAN BEING. WRITE YOUR SOLUTIONS NEATLY AND COHERENTLY, OR THEY RISK NOT RECEIVING FULL CREDIT
THIS EXAM WILL BE ELECTRONICALLY SCANNED. MAKE SURE YOU WRITE ALL SOLUTIONS IN THE SPACES PROVIDED. YOU MAY WRITE SOLUTIONS ON THE BLANK PAGE AT THE BACK BUT BE SURE TO CLEARLY LABEL THEM

Name: Alex Paulin

This exam consists of 7 questions. Answer the questions in the spaces provided.

1. (25 points) (a) Carefully define what it means for a set R to be a field. State all the axioms precisely. Give two examples of a field, neither of which is contained in the other.

Solution:

A field is a set, R, equipped with two binary operations $+$ and $\times$, such that

1/ $|R| > 1$

2/ $(a+b)+c = a+(b+c) \quad \forall a,b,c \in R$

3/ $\exists\, 0_R \in R$ s.t. $0_R + a = a + 0_R = a \quad \forall a \in R$

4/ Given $a \in R$, $\exists\, b \in R$ s.t. $a+b = b+a = 0_R$

5/ $a+b = b+a \quad \forall a,b \in R$

6/ $a \times (b \times c) = (a \times b) \times c \quad \forall a,b,c \in R$

7/ $\exists\, 1_R \in R$ s.t. $1_R \times a = a \times 1_R = a \quad \forall a \in R$

8/ $a \times b = b \times a \quad \forall a,b \in R$

9/ $a \times (b+c) = a \times b + a \times c \quad \forall a,b,c \in R$

10/ Given $a \in R \setminus \{0_R\}$, $\exists\, b \in R$ s.t. $a \times b = 1_R$

(b) Prove that a field is an integral domain. If you use any result from lectures be sure to state it clearly.

Solution:

Let R be a field $\Rightarrow$ R is non-trivial and commutative

Let $a, b \in R$ s.t. $ab = 0_R$.

Assume $a, b \neq 0_R \Rightarrow a, b \in R^* \Rightarrow \exists\, a^{-1}, b^{-1} \in R$

$\Rightarrow abb^{-1}a^{-1} = 0_R b^{-1}a^{-1} \Rightarrow 1_R = 0_R$

$\Rightarrow R$ trivial. Contradiction.

Hence either $a = 0_R$ or $b = 0_R$ $\Rightarrow$ R an I.D.

(c) Is the converse to b) true? Be sure to justify your answer.

Solution:

No, the converse is not true.

E.g. $\mathbb{Z}$ is an I.D. but not a field.

2. (25 points) Let R and S be non-trivial rings and $\phi : R \to S$ be a ring homomorphism.

   (a) Define $ker(\phi) \subset R$ and prove it is an ideal. You do not need to prove it is a subgroup under addition.

   Solution:

$\ker\phi = \{a \in R \mid \phi(a) = 0_R\} \subset R$. Because ϕ is a group homomorphism under $+$ we know $(\ker\phi, +)$ is a subgroup of $(R, +)$. Let $r \in R$, $a \in \ker\phi \Rightarrow$

$\phi(ra) = \phi(r)\phi(a) = \phi(r)0_R = 0_R \Rightarrow ra \in \ker\phi$

$\phi(ar) = \phi(a)\phi(r) = 0_R\,\phi(r) = 0_R \Rightarrow ar \in \ker\phi$ $\Rightarrow \ker\phi$ an ideal

   (b) Prove that $ker(\phi) \subset R$ is not a subring. You may assume any results from the lectures as long as they are clearly stated.

   Solution:

$\ker\phi \subset R$ a subring $\Rightarrow 1_R \in \ker\phi \Rightarrow \phi(1_R) = 0_S = 1_S$

$\Rightarrow S$ trivial. Contradiction.

$\Rightarrow 1_R \notin \ker\phi \Rightarrow \ker\phi$ not a subring of R

   (c) Prove that if R is a field then R is isomorphic to a subring of S. You may assume any results from the lectures as long as they are clearly stated

   Solution:

R Field $\Rightarrow$ only ideals are $\{0_R\}$ and R

$\ker\phi \neq R$ by b). $\Rightarrow \ker\phi = \{0_R\} \Rightarrow \phi$ injective

$\Rightarrow R \cong \operatorname{Im}\phi \subset S$.

3. (25 points) Let R be a commutative ring

(a) Define what it means for an ideal $I \subset R$ to be prime.

Solution:

$I \subset R$ is a prime ideal if

1/ $I \neq R$

2/ $ab \in R \Rightarrow a \in I$ or $b \in I$

(b) Prove that R/I is an integral domain if and only if I is prime.

Solution:

$(\Rightarrow)$ R/I integral domain $\Rightarrow$ R/I non-trivial $\Rightarrow I \neq R$

Let $a, b \in R$ and $ab \in I$. $\Rightarrow ab + I = 0_R + I$

$\Rightarrow (a+I)(b+I) = 0_R + I \Rightarrow a + I = 0_R + I$ or

$b + I = 0_R + I \Rightarrow a \in I$ or $b \in I \Rightarrow I$ prime

$(\Leftarrow)$ I prime $\Rightarrow I \neq R \Rightarrow R/I$ non-trivial

Let $a, b \in R$ and $(a+I)(b+I) = 0_R + I \Rightarrow ab \in I$

$\Rightarrow a \in I$ or $b \in I \Rightarrow a + I = 0_R + I$ or $b + I = 0_R + I$

$\Rightarrow R/I$ integral domain

(c) Give an example of a prime ideal which is not maximal.

Solution:

$\{0\} \subset \mathbb{Z}$ is prime ($\mathbb{Z}$ is an I.D.)

It is not maximal as $(0) \subsetneq (2) \subsetneq \mathbb{Z}$.

4. (25 points) Let R be an integral domain.

   (a) Define what is means for R to be UFD.

   Solution:

R is a UFD if

1/ Every non-zero, non-unit can be written as a product of irreducibles

2/ If $a_1 \dots a_n = b_1 \dots b_m$, b_i, a_j irreducible $\Rightarrow n = m$ and (after reordering) a_i associated to b_i $\forall i$.

   (b) Define what it means for $r \in R$ to be prime. Prove that r prime $\Rightarrow$ r irreducible.

   Solution:

$r \in R$ prime if 1/ $r \neq 0_R$, 2/ $r \notin R^*$, 3/ $r | ab \Rightarrow r | a$ or $r | b$

Assume $r = ab \Rightarrow r | ab \Rightarrow r | a$ or $r | b$. WLOG assume $a = rk \Rightarrow r = rkb \Rightarrow 1_R = kb \Rightarrow b \in R^*$

$\Rightarrow$ r is irreducible.

   (c) Prove that in a UFD, r irreducible $\Rightarrow$ r prime.

Let $r \in R$ be irreducible, and $r | ab \Rightarrow rk = ab$ for $k \in R$. $a = 0_R \Rightarrow r | a$, $b = 0_R \Rightarrow r | b$. Assume $a, b \neq 0_R$

$a \in R^* \Rightarrow rka^{-1} = b \Rightarrow r | b$

$b \in R^* \Rightarrow rkb^{-1} = a \Rightarrow r | a$

$a, b \notin R^* \Rightarrow rk = \underbrace{a_1 \dots a_n}_{= a} \underbrace{b_1 \dots b_m}_{= b}$ where a_i, b_j irreducible.

2/ $\Rightarrow r | a_i$ for some i or $r | b_j$ for some j

$\Rightarrow r | a$ or $r | b$.

$\Rightarrow$ r prime.

5. (25 points) Let F be a field, $\alpha \in F$ and $f(x) \in F[x]$ such that $deg(f(x)) \geq 1$. Prove $f(\alpha) = 0_F \iff (x-\alpha)|f(x)$ in $F[x]$. You may assume any results from lectures as long as they are clearly stated. If $f(x) \in F[x]$ reducible is it true that $\exists\, \alpha \in F$ s.t. $f(\alpha) = 0$

Solution:

$(F[x], deg)$ Euclidean $\Rightarrow f(x) = q(x)(x-\alpha) + r(x)$
$q(x), r(x) \in F[x]$

where $r(x) = 0_{F[x]}$ or $deg(f(x)) = 0$

$(\Rightarrow)$ $f(\alpha) = 0_F \Rightarrow q(\alpha)(\alpha - \alpha) + r(\alpha) = 0_F$

$\Rightarrow r(\alpha) = 0_F \Rightarrow r(x) = 0_{F[x]} \Rightarrow (x-\alpha) | f(x)$.

$(\Leftarrow)$ $(x-\alpha) | f(x) \Rightarrow f(x) = (x-\alpha)\, q(x)$, $q(x) \in F[x]$

$\Rightarrow f(\alpha) = (\alpha - \alpha) q(\alpha) = 0_F\, q(\alpha) = 0_F$.

$f(\alpha) = 0_F$ for some $\alpha \in F \not\Leftarrow f(x)$ irreducible

E.g. $(x^2+1)^2 \in \mathbb{R}[x]$ is reducible and $\nexists\, \alpha \in \mathbb{R}$

s.t. $(\alpha^2+1)^2 = 0_{\mathbb{R}}$.

6. (25 points) (a) Define what it means for $f(x) \in \mathbb{Z}[x]$ to be primitive.

Solution:

$f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ primitive if

1) $\deg(f(x)) \geq 1$

2) $a | a_i \ \forall i \Rightarrow a \in \mathbb{Z}^* = \{\pm 1\}$

(b) State, without proof, Gauss' Lemma for polynomials in $\mathbb{Z}[x]$.

Solution:

The product of $\mathbb{Z}$ primitive polynomials is primitive.

(c) Does the polynomial $f(x) = 2x^{11} - 98x^5 + 28x^2 + 35$ have any roots in $\mathbb{Z}$? Is the ~~ring $\mathbb{C}[x]/(f(x))$ a field?~~ ring $\mathbb{Q}[x]/(f(x))$ a field Is the ring $\mathbb{C}[x]/(f(x))$ a field? You may assume any results from lectures as long as they are clearly stated.

Solution:

$f(x) = 2x^{11} - 2\cdot 7^2 x^5 + 2^2 \cdot 7 x^2 + 5 \cdot 7 \in \mathbb{Z}[x]$

By Eisenstein's Criterion with $p = 7$ we see that $f(x)$ is irreducible in $\mathbb{Q}[x]$. If $\alpha \in \mathbb{Z}$ was a root $\Rightarrow f(x) = (x - \alpha) g(x)$, $g(x) \in \mathbb{Q}[x] \Rightarrow f(x)$ reducible.

<u>Contradiction</u>. Hence there are no roots in $\mathbb{Z}$.

$f(x) \in \mathbb{Q}[x]$ irreducible $\Rightarrow (f(x)) \subset \mathbb{Q}[x]$ maximal

$\Rightarrow \mathbb{Q}[x]/(f(x))$ a field.

$\mathbb{C}$ is algebraically closed $\Rightarrow f(x)$ reducible in $\mathbb{C}[x]$

$\Rightarrow (f(x)) \subset \mathbb{C}[x]$ <u>not</u> maximal $\Rightarrow \mathbb{C}[x]/(f(x))$ <u>not</u> a field.

7. (25 points) (a) Let E/F be a field extension. Define what if means for $\alpha \in E$ to be algebraic over F.

Solution:

$\alpha \in E$ is algebraic if $\exists\, f(x) \in F[x]$, non-constant, such that $f(\alpha) = 0_F$.

(b) Prove that $\sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

Solution:

$\alpha = \sqrt{2} + \sqrt{3} \Rightarrow \alpha^2 = 2 + 3 + 2\sqrt{2}\sqrt{3} = 5 + 2\sqrt{6}$

$\Rightarrow \alpha^2 - 5 = 2\sqrt{6} \Rightarrow (\alpha^2 - 5)^2 = 24$

$\Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0$

Let $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$

$f(x)$ non-constant and $f(\sqrt{2} + \sqrt{3}) = 0$

$\Rightarrow \sqrt{2} + \sqrt{3}$ algebraic over $\mathbb{Q}$

(c) Using this, or otherwise, prove that if $\alpha \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, then there exists $f(x) \in \mathbb{Q}[x]$ non-zero, such that $deg(f(x) \leq 4$ and $f(\alpha) = 0$. You may assume any results from lectures as long as they are clearly stated.

Solution:

Let $h(x) \in \mathbb{Q}[x]$ be min poly of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$

$\Rightarrow h(x) \mid x^4 - 10x^2 + 1 \Rightarrow \deg h(x) \leq 4$

$\Rightarrow [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \leq 4$

If $\alpha \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \Rightarrow \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \leq 4$

$\Rightarrow$ Min polynomial of α over $\mathbb{Q}$ has degree ≤ 4

$\Rightarrow \exists\, f(x) \in \mathbb{Q}[x]$, non-constant, $\deg(f(x)) \leq 4$
s.t. $f(\alpha) = 0$

END OF EXAM