MATH 113 FINAL EXAM (PRACTICE 1)

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 ring. State all the axioms precisely.

Solution:

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

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

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

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

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

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

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

7/ $a\times(b+c) = a\times b + a\times c$ <u>and</u> $(a+b)\times c = a\times c + b\times c$ $\forall a,b,c \in R$

(b) Define the units $R^* \subset R$.

Solution:

$R^* = \{a \in R \mid \exists\, b \in R \text{ s.t. } a\times b = b\times a = 1_R\}$

(c) Prove, using only the axioms, that $R^* = R$ implies that $|R| = 1$.
Solution:

Claim $0_R a = 0_R \quad \forall a \in R$

Proof $0_R a = (0_R + 0_R) a = 0_R a + 0_R \Rightarrow 0_R a = 0_R$ $\square$

$R^* = R \Rightarrow 0_R \in R^* \Rightarrow \exists\, b \in R$ s.t.

$0_R = 0_R \cdot b = 1_R$

Claim : $0_R = 1_R \Rightarrow |R| = 1$

Proof : Let $a \in R$. Then $0_R = 0_R \cdot a = 1_R \cdot a = a$

$\Rightarrow |R| = 1$

Hence $R^* = R \Rightarrow |R| = 1$

2. (25 points) Let R be a ring.

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

Solution:

$I \subset R$ is an ideal if

1/ I is a subgroup of R under addition

2/ $x \in I$, $r \in R \Rightarrow rx, xr \in I$

(b) Prove that the binary operation

$$\begin{aligned} \phi : R/I \times R/I &\longrightarrow R/I \\ (x+I, y+I) &\longrightarrow (xy)+I \end{aligned}$$

is well-defined, i.e. independent of coset representative choices.

Solution:

Let $x_1, x_2, y_1, y_2 \in R$ s.t. $x_1 + I = x_2 + I$ and $y_1 + I = y_2 + I$

$\Rightarrow$ $x_1 - x_2 \in I$ and $y_1 - y_2 \in I$

$x_1 y_1 - x_2 y_2 = x_1 \underbrace{(y_1 - y_2)}_{\in I} + \underbrace{(x_1 - x_2)}_{\in I} y_2$

I ideal $\Rightarrow$ $x_1 y_1 - x_2 y_2 \in I$ $\Rightarrow$ $x_1 y_1 + I = x_2 y_2 + I$

$\Rightarrow$ ϕ is well defined

(c) If R/I is the quotient ring, is the following true:
$x + I \in (R/I)^* \Rightarrow x \in R^*$. Be sure to justify your answer.

Solution:

maximal

No. Example $R = \mathbb{C}[x]$, $I = (x+1)$

$\Rightarrow$ $\mathbb{C}[x]/(x+1)$ a field and $x + (x+1) \neq 0 + (x+1)$

Hence $x + (x+1) \in \left(\mathbb{C}[x]/(x+1)\right)^*$ but $x \notin (\mathbb{C}[x])^*$

3. (25 points) Let R be an integral domain.

(a) Define the characteristic of R.

Solution:

$\mathrm{Char}(R) = 0 \iff \mathrm{ord}_+(1_R) = \infty$

$\mathrm{Char}(R) = p \iff \mathrm{ord}_+(1_R) = p$

(b) Prove that if the characteristic of R is p, then there is an injective homomorphism $\phi : \mathbb{F}_p \to R$. Be sure to carefully justify your answer.

Define $\phi : \mathbb{F}_p \longrightarrow R$

$[a] \longrightarrow a 1_R$

Claim: ϕ is well defined.

Proof: $[a] = [b] \Rightarrow a - b = pk \Rightarrow (a-b)1_R = k(p 1_R) = 0_R$

$\Rightarrow a 1_R = b 1_R$

Claim: ϕ is a ring homomorphism

$\phi([a]+[b]) = (a+b)1_R = a 1_R + b 1_R = \phi([a]) + \phi([b])$

$\phi([a][b]) = (ab) 1_R = (a 1_R)(b 1_R) = \phi([a])\phi([b])$

$\phi([1]) = 1 \cdot 1_R = 1_R$

Claim: ϕ is injective

Proof: $\ker \phi = \{ [a] \mid a 1_R = 0_R \}$. $\mathrm{ord}_+(1_R) = p \Rightarrow$

$\ker \phi = \{ [a] \mid p \mid a \} = \{[0]\} \Rightarrow \phi$ injective

$\square$

4. (25 points) Let R be a commutative ring.

   (a) Define what it means for two elements $a, b \in R$ to be associated.

   Solution:

$a, b \in R$ are associated $\iff$ $a \mid b$ <u>and</u> $b \mid a$

   (b) Prove that if R is an integral domain then a and b both non-zero are associated if and only if there exists $u \in R^*$ such that $a = ub$.

   Solution:

Let $u \in R^*$ s.t. $a = ub \Rightarrow b = u^{-1}a \Rightarrow a \mid b$ <u>and</u> $b \mid a$

Assume $a \mid b$ <u>and</u> $b \mid a \Rightarrow \exists\ c, d \in R$ s.t. $a = bc$, $b = ad$

$\Rightarrow a = adc \Rightarrow 1 = dc \Rightarrow c \in R^*$

   (c) Using this, prove that $2\sqrt{2} + 1$ and $5 + 3\sqrt{2}$ are associated in $\mathbb{Z}[\sqrt{2}]$.

$$\frac{5 + 3\sqrt{2}}{2\sqrt{2}+1} = 5 + 3\sqrt{2} \cdot \frac{1}{1 + 2\sqrt{2}} = (5 + 3\sqrt{2}) \cdot \frac{1 - 2\sqrt{2}}{(1 + 2\sqrt{2})(1 - 2\sqrt{2})}$$

$$= \frac{(5 + 3\sqrt{2}) \cdot (1 - 2\sqrt{2})}{-7} = \frac{5 - 12 + 3\sqrt{2} - 10\sqrt{2}}{-7}$$

$$= 1 + \sqrt{2}$$

$$(\sqrt{2}+1)(\sqrt{2}-1) = 1 \Rightarrow 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$$

$$\Rightarrow (5 + 3\sqrt{2}) = (2\sqrt{2} + 1)\underset{\substack{\uparrow \\ (\mathbb{Z}[\sqrt{2}])^*}}{(1 + \sqrt{2})} \Rightarrow 5 + 3\sqrt{2},\ 2\sqrt{2} + 1 \text{ are associated}$$

5. (25 points) Prove that if R is a PID then $a \in R$ non-zero is irreducible $\iff$ $(a) \subset R$ is maximal.

Solution:

Let R be a P.I.D.

($\Rightarrow$) a irreducible $\Rightarrow$ $a \notin R^*$ $\Rightarrow$ $(a) \subsetneq R$ (ie (a) is proper)

Let $(a) \subset I \subset R$, I an ideal.

R a P.I.D. $\Rightarrow$ $I = (b)$ for some $b \in I$ $\Rightarrow$

$(a) \subset (b)$ $\Rightarrow$ $b \mid a$ $\Rightarrow$ $a = bc$ $\Rightarrow$ $b \in R^*$ or $c \in R^*$

$$\left.\begin{array}{l} b \in R^* \Rightarrow (b) = I = R \\ c \in R^* \Rightarrow (a) = (b) \end{array}\right\} (a) \subset R \text{ is maximal}$$

($\Leftarrow$) Let $(a) \subset R$ be maximal $\Rightarrow$ $a \notin R^*$

Assume $a = bc$ $\Rightarrow$ $(a) \subset (b) \subset R$

$$\left.\begin{array}{l} (a) = (b) \Rightarrow c \in R^* \\ R = (b) \Rightarrow b \in R^* \end{array}\right\} a \text{ is irreducible}$$

6. (25 points) Let R be an integral domain.

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

   Solution:

$I \subset R$ is maximal if

1/ It is proper i.e. $I \neq R$

2/ $I \subseteq J \subseteq R$, J an ideal $\Rightarrow I = J$ or $J = R$

   (b) Is the ideal $(x^4 - 1, x^5 - x^3) \subset \mathbb{Q}[X]$ maximal? Be sure to carefully justify your answer. If you use any results from lecture be sure to state them clearly.

   Solution:

Facts: $\mathbb{Q}$ field $\Rightarrow \mathbb{Q}[x]$ Euclidean $\Rightarrow \mathbb{Q}[x]$ a P.I.D. $\Rightarrow \mathbb{Q}[x]$ a UFD

$x^4 - 1 = (x^2-1)(x^2+1) = (x+1)(x-1)(x^2+1)$ ← irreducible factorization

$x^5 - x^3 = x \cdot x \cdot (x+1)(x-1)$ ← irreducible factorization

$\Rightarrow$ HCF$(x^4-1, x^5-x^3) = (x+1)(x-1)$

$\mathbb{Q}[x]$ Euclidean $\Rightarrow (x+1)(x-1) = f(x)(x^4-1) + g(x)(x^5-x^3)$

for some $f(x), g(x) \in \mathbb{Q}[x]$

$\Rightarrow (x^4-1, x^5-x^3) = ((x+1)(x-1)) \subset \mathbb{Q}[x]$

$(x+1)(x-1)$ not irreducible $\Rightarrow ((x+1)(x-1))$ not maximal.

7. (25 points) (a) Let E/F be a field extension and let $\alpha \in E$ be algebraic over F. Define the minimal polynomial of α over F.

Solution:

Min polynomial of α over F is the monic, non-constant polynomial $f(x)$ of minimal degree such that $f(\alpha) = 0_F$

(b) Prove the minimal polynomial is irreducible.

Solution:

1/ $f(x)$ min polynomial $\Rightarrow \deg(f(x)) \geq 1 \Rightarrow f(x) \neq 0_{F[x]}$

$f(x) \notin (F[x])^*$

2/ Assume $f(x) = g(x)\,h(x)$ with $\deg(g(x)), \deg(h(x)) < \deg(f(x))$

$g(x), h(x) \neq 0_{F[x]}$

$\Rightarrow f(\alpha) = g(\alpha)h(\alpha) = 0_F \Rightarrow$ either $g(\alpha) = 0_F$ or $h(\alpha) = 0_F$

WLOG assume $g(\alpha) = 0_F$. Let $\lambda \in F^*$ s.t. $\lambda g(x)$ monic. Then $\lambda g(\alpha) = \lambda 0_F = 0_F$ and $\deg(\lambda g(x)) = \deg(g(x)) < \deg(f(x))$

Contradiction by minimality of $\deg(f(x))$

$\Rightarrow f(x)$ irreducible

(c) Determine the degree of the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. You may use any results from lectures as long as they are clearly stated.

Let $f(x) = x^3 - 2$. $f(\sqrt[3]{2}) = 0 \Rightarrow$

Minimal polynomial of $\sqrt[3]{2}$ divids x^3-2.

$\deg(x^3-2) = 3 \Rightarrow$ If x^3-2 is reducible it has a root in $\mathbb{Q}$. x^3-2 monic $\Rightarrow$ all rational roots must be in $\mathbb{Z}$. x^3-2 has no roots in $\mathbb{Z} \Rightarrow$

x^3-2 is irreducible in $\mathbb{Q}[x]$.

$\Rightarrow$ x^3-2 is minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$

$$\Rightarrow \quad \mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$$

field because x^3-2 irreducible

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

$$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

END OF EXAM