Name————————————, ID ——————

Exam II: MTH 420, Spring 2018

Ayman Badawi Taha Ameen 60/60

QUESTION 1. Let R be a finite commutative ring with 1. Assume that $AB = \{0\}$ for some maximal ideals A, B of R.

(i) Prove that $|R| = p_1^n p_2^m$ for some prime numbers p_1, p_2 and for some integers n, m.

(ii) (up to isomorphism), describe the structure of R.

(iii) How many maximal ideals does R have?

QUESTION 2. (i) Let E be an integral domain such that $char(E) = 0$. Prove that E has a subring F that is ring-isomorphic to Z (Hint: As I explained in class, construct a ring-homomorphism from Z into E that is one to one, note that now we can conclude that Z is the smallest integral domain that has characteristic equals 0)

(ii) Let F be a field such that $char(F) = 0$. Prove that F has a subfield L such that L is ring-isomorphic to Q. (note write $a/b = ab^{-1}$ for some a, b in Z, $b \neq 0$ and see my hint above. Hence we conclude that Q is the smallest field that has characteristic 0)

(iii) Prove that the identity map from Z ONTO Z is the only ring-isomorphism from Z ONTO Z

(iv) Prove that the identity map from Q ONTO Q is the only ring-isomorphism from Q ONTO Q

QUESTION 3. (as I promised in class). Let $F \subset E$ be fields extension such that E is a finite field. Prove that E is ring-isomorphic to $F[x]/(f(x))$ for some monic irreducible polynomial $f(x)$ over F that satisfies $f(a) = 0$, where $(E^*, .) =< a >$.

QUESTION 4. (JUST BEAUTIFUL !!!!)

(i) Let $E = GF(p^n)$. Prove that every monic IRREDUCIBLE polynomial of degree n over Z_p splits completely in E. (Hint: let $f(x) = x^n + ... + a_1x + a_0$ be a monic irreducible polynomial of degree n over Z_p. We know that $f(x)$ splits completely in $F = Z_p[x]/(f(x))$. Note $|F| = |E|$. Thus F is ring-isomorphic to E. Let $L : F \rightarrow E$ be a ring-isomorphism. Show that $L(a) = a$ for every $a \in Z_p$. Now let b in F such that $f(b) = b^n + ... + a_1b + a_0 = 0$. Show that f(L(b)) = 0. Hence $L(b)$ is a root of $f(x)$.)

(ii) (WAW ! indeed) Fix an integer k and a prime number p. Let $h = p^k$. Prove that the product of ALL monic IRREDUCIBLE polynomials over Z_p whose degrees divide k is equal to $f(x) = x^h - x$ (hint: We know that $GF(p^d)$ is a subfield of $GF(p^k)$ if and only if $d \mid k$. Now use (i) and the fact that $f(x)$ splits completely in $GF(p^k)$ and it has no multiple roots and $f(x)$ has exactly p^k roots,)

(iii) (NICE!, calculation) Let p be a prime number

a. Find the number of all ALL monic irreducible polynomials of degree 2 over Z_p. (hint: Consider $E = GF(p^2)$ and use (ii))

b. Find the number of all ALL monic irreducible polynomials of degree 3 over Z_p. (hint: Consider $E = GF(p^3)$ and use (ii))

c. Let b be a prime number. Find the number of all ALL monic irreducible polynomials of degree b over Z_p. (hint: Consider $E = GF(p^b)$ and use (ii))

d. Find the number of all ALL monic irreducible polynomials of degree 4 over Z_p. (hint: Consider $E = GF(p^4)$, use (ii), and note that you already know the number of all ALL monic irreducible polynomials of degree 2 over Z_p.)

e. Find the number of all ALL monic irreducible polynomials of degree 8 over Z_p. (hint: Consider $E = GF(p^8)$, use (ii), and note that you already know the number of all ALL monic irreducible polynomials of degrees 2 and 4 over Z_p.)

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com

ANSWER 2: E is an Integral domain with $\text{char}(E) = 0$.

(i) **To Show:** $\exists\ F \subset E$ s.t. F is a Subring of E and $F \approx \mathbb{Z}$.

Proof: Consider $f : \mathbb{Z} \longrightarrow E$ s.t. $f(m) = m \cdot 1_E$

i.e. $f(m) = \underbrace{1_E + 1_E + \dots + 1_E}_{m \text{ times}}$.

Then f is a ring homomorphism

$\longrightarrow f(m+n) = (m+n)\cdot 1_E = m \cdot 1_E + n \cdot 1_E = f(m) + f(n)$

$\longrightarrow f(m \cdot n) = (m * n) \cdot 1_E = m \cdot 1_E * n \cdot 1_E = f(m) \cdot f(n)$

We show f is one-to-one by showing $\ker(f) = \{0\}$.

DENY. $\therefore \exists\, l \in \mathbb{Z}$ s.t. $f(l) = 0$.

$\therefore f(l) = 0 \implies l \cdot 1_E = 0 \implies \text{char}(E) \neq 0$

CONTRADICTION.

4/4

Let F be the Image of f.

Then $\dfrac{\mathbb{Z}}{\ker(f)} \approx \text{Im}(f) \implies \dfrac{\mathbb{Z}}{\{0\}} \approx F \implies \mathbb{Z} \approx F$

and F is a Subring of E. $\blacksquare$

(ii) **To Show:** When F is a field with $\text{char}(F) = 0$,

Show $\exists\ L \subset F$ s.t. L is a Subfield of F and $L \approx \mathbb{Q}$.

Proof: Consider $f : \mathbb{Q} \longrightarrow F$

s.t. $f\left(\dfrac{a}{b}\right) = \dfrac{a * 1_F}{b * 1_F} = a * 1_F * (b * 1_F)^{-1}$

Then f is a ring homomorphism

$\longrightarrow f\left(\dfrac{a}{b} + \dfrac{c}{d}\right) = f\left(\dfrac{ad+bc}{bd}\right) = (ad+bc)*1_F * (bd * 1_F)^{-1}$

$= (ad * 1_F + bc * 1_F) * (b * 1_F)^{-1} \cdot (d * 1_F)^{-1}$

$= (a * 1_F * d * 1_F + b * 1_F * c * 1_F) * (b * 1_F)^{-1} * (d * 1_F)^{-1}$

$$= (a * 1_F) * (d * 1_F) * (d * 1_F)^{-1} * (b * 1_F)^{-1} + (b * 1_F) * (b * 1_F)^{-1} * (c * 1_F) * (d * 1_F)^{-1}$$

$$= (a * 1_F) * (b * 1_F)^{-1} + (c * 1_F) * (d * 1_F)^{-1}$$

$$= f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right)$$

$$\longrightarrow f\left(\frac{a}{b} * \frac{c}{d}\right) = f\left(\frac{ac}{bd}\right) = (ac * 1_F) * (bd * 1_F)^{-1}$$

$$= (a * 1_F) * (c * 1_F) * (b * 1_F)^{-1} * (d * 1_F)^{-1}$$

4/4

$$= (a * 1_F) * (b * 1_F)^{-1} * (c * 1_F) * (d * 1_F)^{-1}$$

$$= f\left(\frac{a}{b}\right) * f\left(\frac{c}{d}\right)$$

We show: f is One-to-One. by showing $\ker(f) = \{0\}$.

Deny. $\therefore \exists \frac{m}{n} \in \mathbb{Q}$ s.t. $f\left(\frac{m}{n}\right) = 0$ and $m \neq 0$.

Then $f\left(\frac{m}{n}\right) = (m * 1_F) * (n * 1_F)^{-1} = 0$.

Since F is a field (and hence an Integral domain), we have $m * 1_F = 0$ or $n * 1_F = 0$ $\left(\begin{matrix} n \neq 0 \\ m \neq 0 \end{matrix}\right)$

This contradicts $\text{char}(F) = 0$.

Contradiction!

$\therefore$ Let $L = \text{Im}(f)$

$$\Longrightarrow \frac{\mathbb{Q}}{\{0\}} \approx L \Longrightarrow \mathbb{Q} \approx L \quad \text{(By First Isomorphism Theorem)}$$

We show: L is a field.

- Clearly, $1_F \in L$. $\left(\because \exists \frac{1}{1} \in \mathbb{Q} \text{ s.t. } f\left(\frac{1}{1}\right) = 1_F\right)$.
- $\forall \frac{a * 1_F}{b * 1_F} \in L \;\; \exists \frac{b * 1_F}{a * 1_F} = f\left(\frac{b}{a}\right) \in L$ s.t. $\left(\frac{a * 1_F}{b * 1_F}\right)\left(\frac{b * 1_F}{a * 1_F}\right) = 1_F$

$\therefore \forall u \in L \;\; \exists u^{-1} \in L \Longrightarrow L$ is a Field.

(iii) <u>To show:</u> $\forall a \in \mathbb{Z}$, $f(a) = a$ is the Only Ring Isomorphism from $\mathbb{Z}$ onto $\mathbb{Z}$.

<u>Proof:</u> <u>Deny.</u> $\therefore f(1) \neq 1. \implies$ Let $f(1) = k$, $k \in \mathbb{Z}$.

$\therefore f(1^2) = [f(1)]^2 \implies f(1) = f(1) \cdot f(1)$

$\therefore k = k^2 \implies k(k-1) = 0.$

Since $\mathbb{Z}$ is an Integral domain, $k=0$ OR $k=1$

By Assumption, $k \neq 1$. $\therefore k = 0$. But, this is the trivial map and is not an Isomorphism.

Contradiction.

$\therefore f(1) = 1.$

<u>Now:</u> <u>To prove:</u> $f(1) = 1 \implies f(n) = n$. <u>Case 1:</u> $n \geq 1$

By Math Induction: Assume $f(k) = k$.

Then $f(k+1) = f(k) + f(1) = k+1$.

Since $f(1) = 1 \implies f(n) = n \quad \forall n \geq 1$.

4/4

<u>Case 2:</u> $n < 0$ Clearly, $f(0) = 0$.

$\therefore f(n + -n) = f(n) + f(-n) = 0 \implies f(n) = -f(-n)$

Since $-n > 0$, we have $f(n) = -(-n) = n$

$\therefore f(n) = n \quad \forall n$ ∎

(iv). By Same Logic as (iii), we have $f(1) = 1$.

<u>To show:</u> $f\left(\frac{p}{q}\right) = \frac{p}{q} \quad \forall \frac{p}{q} \in \mathbb{Q}$.

Since $q * \frac{p}{q} = p$ and $q \in \mathbb{Z}$, we have:

$$q * f\left(\frac{p}{q}\right) = f(q) * f\left(\frac{p}{q}\right) = f\left(q * \frac{p}{q}\right) = f(p) = p. \quad \Big| \because p, q \in \mathbb{Z}$$

$$\therefore \quad q * f\left(\frac{p}{q}\right) = p \implies f\left(\frac{p}{q}\right) = \frac{p}{q}$$

4/4

$\therefore$ The Identity Map is the ONLY Map.

QUESTION 3: Given: $F \subset E$ where E is a finite field.

To Prove: $E \approx \dfrac{F[x]}{(f(x))}$ for some Monic Irreducible polynomial $f(x)$ s.t. $f(a) = 0$ where $\langle a \rangle = (E^*, *)$

Proof: Let $\phi : F[x] \longrightarrow E$ s.t. $\phi(p(x)) = p(a)$

This is a ring homomorphism.

- $\phi((p+q)(x)) = (p+q)(a) = p(a) + q(a) = \phi(p(x)) + \phi(q(x))$.
- $\phi((p*q)(x)) = (p*q)(a) = p(a) * q(a) = \phi(p(x)) * \phi(q(x))$

Claim: The mapping is Onto.

we show: $\forall\, m \in E \ \exists\, k(x) \in F[x]$ s.t. $k(a) = m$

4/4

Since: $m = a^l$ for some l,

Let $k(x) = x^l \implies \phi(k(x)) = k(a) = a^l = m$.

Claim: $Ker(\phi) = (f(x))$ for some Monic Irreducible Polynomial $f(x)$ s.t. $f(a) = 0$.

Clearly, $Ker(\phi) \neq \{0\}$. (Else $F[x] \approx E$ but $F[x]$ is NEVER a field)

$\therefore$ we expect $Ker(\phi)$ to be of the form $(f(x))$, because $F[x]$ is a PID.

→ $f(x)$ must be Irreducible.

DENY. i.e. $f(x) = p(x) * q(x) \Longrightarrow (p(x) * q(x))$ is NOT a prime Ideal.

$\therefore \dfrac{F[x]}{(p(x)q(x))} \approx E \Longrightarrow$ E is not an Integral Domain.

contradiction

$\therefore f(x)$ MUST be Irreducible.

→ $f(x)$ is MONIC.

- Else, $f(x)$ can be made Monic by dividing by the leading coefficient, as all coefficients are from a field.

→ $f(a) = 0$.

$f(x) \in \ker(\phi) \Longrightarrow \phi(f(x)) = 0 \Longrightarrow f(a) = 0$.

$\therefore$ By First Isomorphism Theorem,

$$\frac{F[x]}{(f(x))} \approx E$$ for a Monic Irreducible polynomial $f(x)$.

ANSWER 4: (i) $E = GF(p^n)$. Show that Every Monic Irreducible polynomial of degree n over $\mathbb{Z}_p$ splits in E.

Proof: consider $f(x) = x^n + \ldots + a_1 x + a_0$ where f is IRREDUCIBLE over $\mathbb{Z}_p$. Then f splits completely in $F = \dfrac{\mathbb{Z}_p[x]}{(f(x))}$.

→ clearly, $F \approx E$ (Ring Isomorphism).

$\therefore \exists\, L: F \longrightarrow E$ s.t. L is a ring Isomorphism.

Clearly, $|F| = |E| = p^n \Longrightarrow char(F) = char(E) = p$.

$\therefore \exists\, M \subset F$ and $N \subset E$ s.t. $M \approx N \approx \mathbb{Z}_p$.

(For simple Notation, we say $\mathbb{Z}_p \subset F$ and $\mathbb{Z}_p \subset E$)

$\longrightarrow$ To Show: $L(a) = a \;\; \forall\, a \in \mathbb{Z}_p$.

Clearly $L(1) = 1$ | $\because L(1 * 1) = L(1) = L(1) * L(1)$

If $L(1) = \lambda \Rightarrow \lambda(\lambda - 1) = 0 \Rightarrow \lambda = 1$

$\therefore$ By Induction (from 1 to p) ($\because \mathbb{Z}_p$ is a Field and $\lambda = 0$ is NOT an Isomorphism)

Assume $f(a) = a$ is true

$\Downarrow$

$f(a+1) = f(a) + f(1) = a + 1$.

$\Downarrow$

$f(a) = a \;\; \forall\, a \in \mathbb{Z}_p$.

4/4

$\longrightarrow f(b) = 0 \Longrightarrow f(x) = (x-b) * f_1(x)$ but $f(x)$ is irreducible over $\mathbb{Z}_p \Longrightarrow b \in F \,|\, \mathbb{Z}_p$.

To Show: $f(L(b)) = 0$.

Claim: f maps Root to Root.

Proof: $f(L(b)) = [L(b)]^n + a_{n-1}[L(b)]^{n-1} + \ldots + a_1[L(b)] + a_0$ — $(*)$

Since $a_i \in \mathbb{Z}_p \;\forall\, i$, $\therefore a_i * [L(b)]^i = L(a_i) * [L(b)]^i = L(a_i * b^i)$

since $L(a_i * b^i) + L(a_j * b^j) = L(a_i * b^i + a_j b^j)$,

we have: $(*) = L(b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0) = L(0) = 0$

$\therefore L(b)$ is a root of $f(x)$ ■

(iii) Let p be prime and $k \in \mathbb{Z}$. $h = p^k$.

To show: Product of all Monic Irreducible Polynomials over $\mathbb{Z}_p$ whose degrees divide k $= f(x) = x^h - x$.

Proof: • $f(x)$ has exactly $h = p^k$ roots.

• $\gcd(f(x), f'(x)) = 1 \implies f(x)$ has No Repeated Roots

• $f(x) \in \mathbb{Z}_p \implies f(x)$ Splits completely in $GF(p^k)$.

$\longrightarrow$ Consider d s.t. $d \mid k$. Then $\exists\ GF(p^d) \subseteq GF(p^k)$

It will not be the case that $f(x)$ splits completely in $\mathbb{Z}_{p^d}$. However, in these fields, $f(x)$ can be written as a product of irreducibles of higher degree.

$\therefore f(x) = x^h - x = k_1(x) \cdot k_2(x) * k_3(x) * \dots * k_\ell(x)$

Claim: k_i's are all possible Irreducibles of all degrees that divide k.

Proof: $\rightarrow$ It is clear that k_i's are irreducible

$\rightarrow$ Since $f(x)$ splits in $GF(p^k)$, $\therefore \deg(k_i) \mid p^k \ \forall i$

Since $k_i \neq k_j \ \forall i \neq j$ ($\because \gcd(f(x), f'(x)) = 1$)

$\therefore$ Each Monic Irreducible polynomial (whose degree divides n) occurs once and only once. $\therefore$ Product $= x^h - x$.

(iii)

(a) Let $E = GF(p^2)$.

$\exists$ Exactly p Irreducible, Monic Polynomials of degree 1 over $\mathbb{Z}_p$, namely

$x-0,\ x-1,\ x-2,\ \dots,\ x-(p-1)$.

The product of all of these gives up to an 'x^p' term.

$\therefore$ The remaining degrees will be due to degree 2 polynomials (only other number that divides 2).

$\therefore$ # of Polynomials: $\dfrac{p^2-p}{2}$.

(since total degree: p^2).

Divide by 2 because each deg (2) polynom contributes to the degree by 2.

(b) Let $E = GF(p^3)$.

$\exists$ Exactly p Monic Irreducible polynomials of degree 1 over $\mathbb{Z}_p$ as mentioned above, and their product gives upto degree 'p'.

$\therefore$ # of Polynomials: $\dfrac{p^3-p}{3}$

$\because$ Each polynomial contributes to the degree by 3.

(c) By same reasoning,
# of polynomials: $\dfrac{p^6-p}{6}$.

(d) $E = GF(p^4) \Rightarrow$ Product of all degree 1, 2, 4 polynomials is $x^{p^4}-x$.

Polynomials of degree 1: p.

Polynomials of degree 2: $\dfrac{p^2-p}{2}$

. Product of all Polynomials $\Rightarrow$ Sum of degrees of each

$\therefore$ # of Polynomials of degree 4:

$$\frac{p^4 - p^2}{4}$$

$\because$ All other polynomials contribute to a total degree of p^2.

(e) # of Polynomials of degree 1: p.

$\Rightarrow \underbrace{x + x + \ldots + x}_{p \text{ times}}$

# of Polynomials of degree 2: $\frac{p^2 - p}{2}$

$\underbrace{x^2 + x^2 + \ldots + x^2}_{\frac{p^2-p}{2} \text{ times}} \Rightarrow$ degree $= p^2 - p$

# of Polynomials of degree 4: $\frac{p^4 - p^2}{4}$

$\underbrace{x^4 + x^4 + \ldots + x^4}_{\frac{p^4-p^2}{4} \text{ times}} \Rightarrow$ degree: $p^4 - p^2$

$\therefore$ So far: $\sum$ All degrees $= p^4$.

Since final $f(x)$ has degree 8,

# of polynomials: $\frac{p^8 - p^4}{8}$ //