Name Taha Ameen, ID b00066555

Final Exam: MTH 420, Spring 2018

$\boxed{\text{Taha Ameen}}$

Ayman Badawi

$\frac{68}{70}$

QUESTION 1. (i) Let M be a maximal ideal of a commutative ring R. We know that $M[x]$ is a proper ideal of $R[x]$. Prove that $R[x]/M[x]$ is never a field.

$\frac{R[x]}{M[x]} \approx \frac{R}{M}[x] \longrightarrow$ consider $\phi : R[x] \longrightarrow \frac{R}{M}[x]$.

s.t. $\phi(a_n x^n + \dots + a_1 x + a_0) = (a_n + M)x^n + \dots + (a_1+M)x + (a_0+M)$

Then: ϕ is a Ring homomorphism.

ϕ is Onto

$Ker(\phi) = M[x]$ | $\because a_i + M = 0 + M \Rightarrow a_i \in M \ \forall i$

$\therefore \frac{R[x]}{M[x]} \approx \frac{R}{M}[x]$

But; Polynomial rings are never fields.

($\exists \ (1+M)x \in \frac{R}{M}[x]$ s.t. $1+M \notin U(\frac{R}{M}[x])$)

$\therefore \frac{R[x]}{M[x]}$ is never a field. ■

4/4

(ii) We know that every prime element of an integral domain is irreducible. Let R be a commutative ring with exactly one maximal ideal (note that R needs not be an integral domain). Prove that every prime element is irreducible. (Hint: you may need to use the fact that $1 + a \in U(R)$ for every $a \in J(R)$)

$\longrightarrow$ The Only Maximal Ideal of R is $J(R)$ | $\because J(R) = \bigcap_{\forall i} M_i = M$

Let 'a' be prime Element. $\therefore a | xy \Rightarrow a|x$ (or) $a|y$.

Also, aR is a prime Ideal.

To Show: a is Irreducible $\Rightarrow$ If $a = xy$, then $x \in U(R)$ (or) $y \in U(R)$.

Proof: $aR \subset J(R)$ | $\because$ Every Ideal is contained in a Maximal Ideal.

$\therefore a \in J(R)$

$xy \Rightarrow a|xy \Rightarrow a|x$ OR $a|y$. If $a|x \Rightarrow x = ak \Rightarrow a = aky$

$\Rightarrow a(1-ky) = 0 \Rightarrow (1-ky) + a(1-ky) = 1-ky \Rightarrow (1+a)(1-ky) = (1-ky)$

and $1+a \in U(R)$ | $\because a \in J(R)$

$\therefore 1-ky = 0 \Rightarrow ky = 1 \Rightarrow y \in U(R)$

($\because$ Unit $\cdot$ something = something)

3/3

(iii) Show that $f(x) = 2x^3 + 5x + 4 \in Z_{10}[x]$ is not a zero-divisor of $Z_{10}[x]$.

Deny. $\therefore \exists \ k \in \mathbb{Z}_{10}^*$ s.t. $k \cdot f(x) = 0$.

But $k \cdot f(x) \neq 0 \ \forall \ k \in \mathbb{Z}_{10}^*$.

(Because $\underbrace{2 * k}_{\text{leading coefficient}} = 0 \Rightarrow k = 5$ but $k = 5 \Rightarrow 5k \neq 0$)

No other option satisfies $2k = 0$.

Contradiction

4/4

$\therefore f(x)$ cannot be a zero divisor.

(iv) Assume that I, J are proper ideals of a commutative ring R. We know that $IJ \subseteq I \cap J$. Assume that I, J are coprime (i.e., there is an $i \in I$ and there is a $j \in J$ such that $i + j = 1$).

a. Show that $I \cap J = IJ$

Let $a \in I \cap J$. To show: $a \in IJ$.

$a \in I \wedge a \in J$. Since I & J are coprime, $\exists i \in I, j \in J$ s.t. $i + j = 1 \Rightarrow ai + aj = a$.

Here: $a \in J$ and $i \in I$, $a \in I$ and $j \in J$ $\Rightarrow$ $ai \in IJ$ and $aj \in IJ$.

$ai + aj \in IJ \Rightarrow a \in IJ$.

$\therefore I \cap J \subseteq IJ$ and $IJ \subseteq I \cap J$.

$\therefore IJ = I \cap J$

5/5

b. Prove that I^m, j^n are coprime for every positive integers n, m, where $1 \le n \le m$. [Hint: Remember the definition of I^k... and stare at the expansion of $(i + j)^k$, also we KNOW that if $a < b$ (positive integers), then $I^b \subseteq I^a$)

Given: I and J are coprime.

$I^m = \sum i_1 i_2 i_3 \ldots i_m$ where $i_j \in I$, and the sum is finite.

First: we show I^k and J^k are coprime. (Same Exponent)

$$(i+j)^k = \underbrace{i^k}_{\in I} + \underbrace{\alpha_1 i^{k-1} j + \alpha_2 i^{k-2} j^2 + \ldots + \alpha_{k-1} i j^{k-1} + j^k}_{\in J} = 1 \quad (\because \exists i, j \text{ st } i + j = 1)$$

5/5

(v) How many polynomials of degree 4 that are units in $Z_9[x]$? $a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$.

$a_0 \in U(\mathbb{Z}_9)$ and $a_i \in Nil(\mathbb{Z}_9)\ \forall i$. Also, $a_4 \neq 0$. Since $\phi(9) = 6$ and $|Nil(\mathbb{Z}_9)| = 3$

Total Choices: $\underset{a_4}{2} * \underset{a_3}{3} * \underset{a_2}{3} * \underset{a_1}{3} * \underset{a_0}{6} = \underline{\underline{324}}$

5/5

(vi) Let $n, m \in Z$ be positive integers > 1 such that $gcd(n, m) = 1$. Let $0 \le a < n$ and $0 \le b < m$. Prove that there is a positive integer $w \in Z$ such that $0 \le w < nm$, $n \mid (w - a)$, and $m \mid (w - b)$ (Hint: Note that nZ, mZ are coprime ideals of Z such that $nZ \cap mZ = nmZ$ and use a theorem that we discussed in class). It should be a very short proof.

$n, m \in \mathbb{Z}$. $\gcd(n, m) = 1$. $0 \le a < n$, $0 \le b < m$.

To Prove: $\exists\ w \in \mathbb{Z}$ s.t. $0 \le w < nm$, $n \mid w - a$, $m \mid w - b$.

Proof: $n\mathbb{Z}$ and $m\mathbb{Z}$ are coprime

$\therefore \dfrac{\mathbb{Z}}{n\mathbb{Z} \cap m\mathbb{Z}} \approx \dfrac{\mathbb{Z}}{n\mathbb{Z}} \times \mathbb{Z}/m\mathbb{Z}$ (C.R.T) $\Rightarrow \mathbb{Z}_{nm} \approx \mathbb{Z}_n \times \mathbb{Z}_m$

Then, let $a \in \mathbb{Z}_n \wedge b \in \mathbb{Z}_m$. $\exists\ w \in \mathbb{Z}_{nm} =$

$\overset{5}{a = 3}$ $\overset{12}{b = 7}$

$w = 21$

$w = \frac{60-21}{39}$

$n \mid w - a$ and $m \mid w - b$

$\therefore \quad w - a = nk_1$ and $w - b = mk_2$

$w = a + nk_1 = b + mk_2$

(vii) Let $f(x,y) = (x+2)y^5 + x^2y^3 + 7x^3y + 10x \in Z[x,y]$. Prove that $f(x,y)$ is irreducible over Z[x]. (Hint: Let $A = Z[x]$. Then Z[x, y] = A[y]. Hence we may view $f(x,y)$ as $K(y)$ a polynomial in terms of y with coefficients from A, and use a theorem!, short proof)

$\mathbb{Z}[x]$ is a UFD $\Rightarrow$ $\mathbb{Z}[x,y]$ is a UFD.

$x \in \mathbb{Z}[x]$ is a prime Element.

$x \nmid (x+2)$, $x \mid x^2$, $x \mid 7x^3$, $x \mid 10x$ AND $x^2 \nmid 10x$.

$\therefore$ By Eisenstein, $f(x,y)$ is Irreducible

5/5

(viii) Give me an example of an integral domain with exactly 3 maximal ideal. Briefly state the steps that are used in order to construct such integral domain

Let $R = \mathbb{Z}$ and $S = \mathbb{Z} \setminus (2\mathbb{Z} \cup 3\mathbb{Z} \cup 5\mathbb{Z})$. Then S is Multiplicatively closed and $R_S = \{ \frac{a}{b} \mid a \in \mathbb{Z} \wedge b \in S \}$ is the required ID

5/5

steps: we can chooses any Q_1, Q_2, Q_3 which are maximal Ideals of $\mathbb{Z}$ and localize $\mathbb{Z}$ over $\mathbb{Z} \setminus Q_1 \cup Q_2 \cup Q_3$.

(ix) Let P be a prime ideal of a commutative ring R and I, J be proper ideals of R such $IJ \subseteq P$. Prove that $I \subseteq P$ or $J \subseteq P$.(Hint: use contradiction). It should be short proof.

P is prime Ideal. $IJ \subseteq P$. To Prove: $I \subseteq P$ (or) $J \subseteq P$.

(*) $IJ \subseteq P \Rightarrow \sum_i ij \in P$ for all finite sums where $i \in I, j \in J$.

Deny: $\therefore I \not\subseteq P$ and $J \not\subseteq P$. But $R \setminus P$ is Multiplicatively closed (Exam 1).

$\therefore i \notin P \wedge j \notin P \Rightarrow ij \notin P$.
This contradicts (*) above.

5/5

(x) Is $\mathbb{R} \subset \mathbb{C}$ a Galois field extension? Find $[\mathbb{C} : \mathbb{R}]$. The Golois group $Gal(C/R)$ is isomorphic to what group? Convince me that every irreducible polynomial over $\mathbb{R}$ is either of degree 1 or 2. (Hint: Let f(x) be an irreducible polynomial of degree n over R, let E be the splitting field of $f(x)$. Then $\mathbb{R} \subset E \subseteq C$. Use class notes $[F_3 : F_1] = [F_3 : F_2][F_2 : F_1]$). Now Prove the well-known fact: Every polynomial of odd degree over $\mathbb{R}$ must have at least one real root (note $\mathbb{R}[x]$ is a UFD!) .

Yes: $\mathbb{R} \subset \mathbb{C}$ is a Galois Field Extension

$[\mathbb{C} : \mathbb{R}] = 2 \because \mathbb{C} \approx \dfrac{\mathbb{R}[x]}{(x^2+1)}$ and $\deg(x^2+1) = 2$.

$\therefore |gal(C/R)| = 2 \Rightarrow gal(C/R) \simeq \mathbb{Z}_2$

$\because$ Every group of prime order $\simeq \mathbb{Z}_p$

$\rightarrow$ To Prove: Every Irreducible polynomial over $\mathbb{R}$ has degree 1 or 2.

From Hint: $\mathbb{R} \subset E \subseteq \mathbb{C} \wedge [\mathbb{C} : \mathbb{R}] = [\mathbb{C} : E] \cdot [E : \mathbb{R}] = 2$.

$\therefore [\mathbb{C} : E] = 2$ and $[E : \mathbb{R}] = 1$ OR $[\mathbb{C} : E] = 1$ and $[E : \mathbb{R}] = 2$

But: E is the splitting field of $\mathbb{R}$. (PTO).

$\therefore$ The Irreducible polynomial in $\mathbb{R}$ which is used to create the Field Extension E such that E is the splitting field of $\mathbb{R}$ has degree 2 OR 1.

$\therefore$ Every Irreducible polynomial must DIVIDE 2 (or) 1

$\Rightarrow$ Every Irreducible polynomial has degree 2 (or) 1. $(E = \mathbb{C})$

$\longrightarrow$ To Prove: Every polynomial of odd degree over $\mathbb{R}$ must have a real root.

Let: $\deg(f(x)) = 2m+1$. consider the Irreducible factorization of f in $\mathbb{R}[x]$.

$$f(x) = (x^2 + a_1x + c_1) * (x^2 + a_2x + c_2) * \dots * (x^2 + a_mx + c_m) * (x + c_{m+1})$$

(OR)

More than 1 $(x + c_k)$ term and lesser $(x^2 + a_kx + c_k)$ terms.

are the ONLY possibilities $(\because \deg(\text{Irreducible}) = 2 \text{ OR } 1.)$

Then, $-c_{m+1} \in \mathbb{R}$ is a root of $f(x)$ $\blacksquare$

QUESTION 2. (i) Let $F = GF(3^3)$ and let m be the number of all monic irreducible polynomials of degree 3 over F (not over Z_3). Find the value of m

$F = GF(3^3)$ and 3 is prime. we look at Monic Irreducibles of degree 3 in $F[x]$.

$\longrightarrow$ Every polynomial over $\mathbb{Z}_3 \subset F$ splits completely in F.

$\therefore$ The Irreducibles have atleast one coefficient from $F/\mathbb{Z}_3$

Since $F \approx$

All elements of F satisfy $x^{3^3} - x = 0$.

$\therefore$ Splitting field of $F = GF(3^9) \Rightarrow x^{3^9} - x = (x^{3^3} - x)(\ldots)$

$\therefore$ # of polynomials : $\dfrac{3^9 - 3^3}{3}$

(ii) Let $F = Z_5$ and let m be the number of all monic irreducible polynomials of degree 4 over F. Find the value of m

By Exam 2 :

$F = \mathbb{Z}_5$ and 5 is prime

$\Downarrow$

Monic Irreducible Polynomials of degree 4 over F

$$\frac{p^4 - p^2}{4} = \frac{5^4 - 5^2}{4} = \underline{\underline{150}}.$$

(iii) Let $F = GF(2^7)$. The the Galois group $Gal(F/Z_2)$ is isomorphic to what group? Find all subfields of F.

Clearly : $[F : \mathbb{Z}_2] = 7$ | $\because F \approx \dfrac{\mathbb{Z}_2[x]}{(f(x))}$ where $\deg(f(x)) = 7$ and f is Monic, Irreducible

$\therefore |Gal(F/\mathbb{Z}_2)| = 7$

$\Longrightarrow Gal(F/\mathbb{Z}_2) \approx \underline{\underline{\mathbb{Z}_7}}$. $H < \mathbb{Z}_7 \Rightarrow H = \mathbb{Z}_7$ OR $H = \{0\}$

$\therefore$ Subfields of F : F AND $\mathbb{Z}_2$.

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