

MTH 532, Exam Two, December 3, 2022, 2:30–4:30 pm

Ayman Badawi

ALL RINGS ARE COMMUTATIVE with $1 \neq 0$

QUESTION 1. (i) **(5 points)** Let $f(x) = x^{40} + 1 \in Z_2[x]$. Then all roots of $f(x)$ "live" inside $F = GF(2^m)$ for some positive integer $m \geq 2$. Find the smallest m, explain briefly. [Hint: Make use of the Freshman Dream Result, note that $-1 = 1$ in Z_2 and $(F^*, .)$ is cyclic.]

Solution: Assume that the smallest field, $F = GF(2^m)$, contains all of the roots of $f(x)$. First, note that $40 = (8)(5) = 2^3(5)$. Hence by the Freshman dream result, $f(x) = x^{40} + 1 = (x^5 + 1)^{2^3}$. Hence, we need to find the roots of $k(x) = x^5 + 1$. Let a be a root of $k(x)$ inside F. Then $a^5 + 1 = 0$. Thus $a^5 = -1 = 1$ in F. Thus the roots of $k(x)$ is the subgroup $D = \{b \in F^* \mid b^5 = 1\}$ of $(F^{,}.)$. Note that $|D| = 5$. Since $(F^*, .)$ is cyclic with $2^m - 1$ elements, we conclude that D is the ONLY subgroup of F^* with 5 element. Hence, by Lagrange Theorem, $5 \mid (2^m - 1)$. Now, by trial and error, find the smallest m such that $5 \mid (2^m - 1)$. It is clear that $m = 4$. Hence $F = GF(2^4)$.

(ii) **(5 points)** Write down all monic irreducible polynomials of degree 2 in $Z_2[x]$.

Solution: By class notes, there is only one such polynomial, $f(x) = x^2 + x + 1$. You may use the formula I gave in class to show that there is only one such polynomials. Since $degree(f) = 2$ and it has no roots in Z_2, $f(x)$ is irreducible by a HW-problem .

(iii) **(5 points)** Convince me that $f(x) = x^4 + x + 1 \in Z_2[x]$is irreducible in $Z_2[x]$. [Hint: Maybe (ii) is useful]

Solution: First observe that $Z_2[x]$ is a UFD (in fact, we know that if F is any field, then $F[x]$ is a PID, and hence a UFD). Deny. Hence $f(x) = k(x)h(x)$. There are two cases. Case one: assume deg(h) = 1 and deg(k) = 3. Since $f(a) \neq 0$ for every $a \in Z_2$, $deg(h) \neq 1$. Case 2: assume $deg(k) = deg(h) = 2$. Since $f(x)$ has no roots in Z_2, we conclude that neither $k(x)$ nor $h(x)$ has roots in Z_2. Thus $k(x)$ and $h(x)$ are irreducible in $Z_2[x]$ by a HW-problem. By (ii), $x^2 + x + 1$ is the only irreducible polynomial of degree 2 in $Z_2[x]$. Thus $k(x) = h(x) = x^2 + x + 1$. Now, $(x^2 + x + 1)^2$ =(by freshman dream) $x^4 + x^2 + 1 \neq f(x)$. Thus our denial is invalid. Hence $f(x) = x^4 + x + 1$ is irreducible in $Z_2[x]$.

(iv) **(5 points)** Given $a \in F = GF(3^{12})$ such that $|a| = 13$ (under multiplication) (i., $a^{13} = 1$ in F). Hence a is a root of a monic irreducible polynomial $f(x)$ in $Z_3[x]$. What is the degree of $f(x)$? explain briefly. [Hint: We know $(F^*, .)$ is cyclic, and hence F^* has exactly once subgroup of order 13.]

Solution: Let $f(x)$ be the monic irreducible polynomial in $Z_3[x]$ of degree m such that $f(a) = 0$. Hence, as explained in the class, m is the smallest degree of such polynomial and $f(x)$ is unique. Thus, by class notes, $Z_3[x]/(f(x)) = GF(3^m)$. Since $a \in GF(3^{12})$, we conclude that $GF(3^m)$ is a subfield of $GF(3^{12})$. Hence $m \mid 12$. Thus $m = 1$, or $m = 2$, or $m = 3$, or $m = 4$, or $m = 6$ or $m = 12$. Since $|a| = 13$, m = the smallest factor of 12 such that $13 \mid (3^m - 1$. By trial and error, $m = 3$. Thus degree(f) = 3)

(v) **(5 points)** How many monic irreducible polynomial of degree 8 are there in $Z_2[x]$? Show the work

Solution: No comments. ALL OF YOU GOT IT RIGHT

(vi) **(5 points)** Write $f(x) = x^9 + x^3 + 2$ as product of monic irreducible polynomials in $Z_3[x]$.

Solution: Since $Z_3[x]$ is a UFD, $f(x)$ can be written uniquely as product of irreducible polynomials in $Z_3[x]$. By staring and the Freshman dream result, $f(x) = (x^3 + x + 2)^3$. If $k(x) = x^3 + x + 2$ is irreducible in $Z_3[x]$, then we are done. Since $k(2) = 0$ in Z_3, we conclude that $k(x)$ is not irreducible in $Z_3[x]$ by a HW-problem. Thus $(x - 2)|k(x)$, note that $(x - 2) = (x + 1)$ in $Z_3[x]$ because $-2 = 1$ in Z_3. Thus $k(x) = (x + 1)h(x)$, where $deg(h) = 2$. By the long division algorithm (i.e., divide $k(x)$ by $(x + 1)$), we conclude that $h(x) = x^2 + 2x + 2$. Since $h(a) \neq 0$ for every $a \in Z_3$, we conclude that $h(x)$ is irreducible. Hence $f(x) = x^9 + x^3 + 2 = \Big((x+1)(x^2+2x+2)\Big)^3 = (x+1)^3(x^2+2x+2)^3$.

(vii) **(5 points)** How many monic irreducible polynomial of degree 6 are there in $Z_2[x]$? Show the work

Solution : No comments, All of you got it right.

QUESTION 2. (10 points) Let $F = GF(2^{12})$. Find $[F : Z_2]$. Find $|Aut_{Z_2}(F)|$. We know that each subgroup of $Aut_{Z_2}(F)$ fixes a unique subfield of F. For each subgroup of $Aut_{Z_2}(F)$, find a generator and the subfield of F that it fixes. Draw a chart that illustrates the relationship between the subgroups of $Aut_{z_2}(F)$ and the subfields of F.

Solution : No comments, All of you got it right.

QUESTION 3. (i) **(5 points)** Let $Q \subset E$ such that $[E : Q] = 21$. Given $f(x)$ is monic irreducible polynomial in $Q[x]$ of degree ≥ 4. If $f(a) = 0$ for some $a \in E$, what are the possibilities of degree(f)? explain briefly

Solution: By class notes, $Q \subset Q(a) \subset E$, where $[Q(a) : Q] = m =$ the degree of $f(x)$. Since $[E : Q] = 21 = [E : Q(a)][Q(a) : Q] = [E : Q(a)]m$, we conclude that $m|21$. Since $m \geq 4$, we conclude that $m = 7$ or $m = 21$.

(ii) **(5 points)** Let $I = \{f(x) \in Z[x] \mid f(1) \in 3Z\}$. We know that $Z[x]$ is a UFD, but not a PID. Convince me that I is a prime ideal of $Z[x]$ and $Z[x]/I$ is a principal ideal domain and hence a UFD [Hint: You can answer this question in ONE step: Construct a ring homomorphism $L : Z[x] \to Z_3$. Then by staring and using some results, you are done.]

Solution: Let $L : Z[x] \to Z_3$ such that $L(f(x)) = f(1)$. We show that L is a ring homomorphism and it is ONTO. $L(k(x) + h(x)) = (k(x) + h(x)(1) = k(1) + h(1) = L(k(x)) + L(h(x))$. $L(k(x)h(x)) = (k(x)h(x))(1) = k(1)h(1) = L(k(x))L(h(x))$ Thus L is a ring homomorphism. Since $L(f(x) = x - 1) = f(1) = 0, L(f(x) = x) = f(1) = 1$, and $L(f(x) = x + 1) = f(1) = 2$. L is onto. Now $Ker(L) = \{h(x) \in Z[x] \mid L(h(x)) = h(1) = 0 \in Z_3\}$. It is clear that $L(h(x)) = h(1) = 0 \in Z_3$ if and only if $h(1) \in 3Z$ Thus $Ker(L) = I$. Hence $Z[x]/I \cong Z_3$. Since Z_3 is a field, I is a maximal ideal of $Z[x]$, and hence it is a prime ideal of $Z[x]$. Since $Z_3 = span\{1\}$ and $\{0\}$ are the only ideals of Z_3, Z_3 is a PID and hence a UFD. Thus $Z[x]/I$ is a PID and a UFD.

(iii) **(5 points)** Let R be a commutative ring with $1 \neq 0$, I be a proper ideal of R, and P be a prime ideal of R such that $I \cap P = \{0\}$. Assume that $ab \neq 0$ for every nonzero elements $a, b \in P$. Convince me that there is a prime ideal W of R such that $I \subseteq W$ and $W \cap P = \{0\}$.

Solution: Let $D = P - \{0\}$. Since P is an ideal of R, $ab \in P$ for every $a, b \in P$. Since $ab \neq 0$ for every nonzero $a, b \in P$, we conclude that $xy \in D$ for every $x, y \in D$. Thus D is a multiplicatively closed set in R. Since $I \cap P = \{0\}$, we conclude that $D \cap I = \emptyset$. Hence, by class-result, there is a prime ideal W of R such that $I \subseteq W$ and $W \cap D = \emptyset$. Since $P = D \cup \{0\}$, we conclude that $W \cap P = \{0\}$.

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`