Name————————————————————————, ID ——————

MTH 532, HW I, WARM UP

Ayman Badawi

QUESTION 1. Solve the following system over Z_8

$$2x + 3y = 0$$

$$x + y = 3$$

sketch: One way eliminate x. Multiply the second equation with the additive inverse of 2, note 6 = -2 is the additive inverse of 2 in Z_8. Hence

$$(1)2x + 3y = 0$$

$$(2)6x + 6y = 2$$

Now add (1) to (2), we get $9y = 2$. Now the multiplicative inverse of $9 = 9^{-1} = 9$. Hence $y = 2$. Substitute $y = 2$ in (1), we get x = 1.

QUESTION 2. Find the inverse of A if possible over Z_{19}

$$A = \begin{bmatrix} 2 & 17 \\ 1 & 1 \end{bmatrix}$$

Sketch $|A| = 2 + -17 = 2 + 2 = 4$. **Hence the inverse of A is** $A^{-1} = 4^{-1}\begin{bmatrix} 1 & 2 \\ 18 & 2 \end{bmatrix} = 5\begin{bmatrix} 1 & 2 \\ 18 & 2 \end{bmatrix} = \begin{bmatrix} 5 & 10 \\ 14 & 10 \end{bmatrix} =$

QUESTION 3. Let $A = \{1, 2, 3, 4\}$ and $R = (P(A), +, .)$, where $+$ and $\,.\,$ as explained in the class.

1) Convince me that R does not have a subring with 6 elements. [short answer : a few lines!, by staring]

Sketch: Let D be a subring of R. Since (R, +) is a group of order 16 and (D, +) is a subgroup of $(R, +)$, the order of every subgroup must be a factor of 16. Since 6 is not a factor of 16, R does not have a subring with 6 elements.

2) Find the inverse of M where

$$M = \begin{bmatrix} \{1, 2\} & \{3, 4\} \\ \{1, 3, 4\} & \{1, 2, 4\} \end{bmatrix}$$

Sketch: $|M| = A \in U(P(A))$

Hence $M^{-1} = AM^{-1}\begin{bmatrix} \{1, 2, 4\} & \{3, 4\} \\ \{1, 3, 4\} & \{1, 2\} \end{bmatrix} = \begin{bmatrix} \{1, 2, 4\} & \{3, 4\} \\ \{1, 3, 4\} & \{1, 2\} \end{bmatrix}$

3) Solve for $x, y \in P(A)$ (if possible), where

$$\{1, 2\}x + \{3, 4\}y = \{2, 4\}$$

$$\{1, 3, 4\}x + \{1, 2, 4\}y = \{1, 2\}$$

Sketch Note that M is the coefficient matrix of the system. Hence

$$\begin{bmatrix} x \\ y \end{bmatrix} = M^{-1}\begin{bmatrix} \{2, 4\} \\ \{1, 2\} \end{bmatrix} = \begin{bmatrix} \{2, 4\} \\ \{1, 2, 4\} \end{bmatrix}$$

QUESTION 4. 1) Let $I = span\{6, 15\}$ over Z, i.e., $I = (4, 6)Z$. We know every ideal of Z is of the form nZ for some integer n. Hence $I = nZ$, find n [Hint: $gcd(a, b) = ca + db$ for some $c, d \in Z$]

Sketch: Since $gcd(6, 15) = 3 = 6a + 15b$ for some $a, b \in R$, we conclude that $3 \in I$. Thus $span\{3\} \subset I$. It is clear that $6 = 3X2 \in span\{3\}$ and $15 = 3X5 \in span3$. Since $span\{3\}$ is an ideal of Z and $6 \in Span\{3\}$ and $15 \in Span\{3\}$, we conclude that $6c + 15d \in span\{3\}$ for every $c, d \in Z$. Thus $span\{3\} = Span\{6, 9\}$

2) Let I, K be ideals of a commutative ring R. Prove $I \cap K$ is an ideal of R. Assume neither $I \subseteq K$ nor $K \subseteq I$. Prove that $I \cup K$ is not an ideal of R.

sketch : Let $x, y \in I \cap K$. Then $x, y \in I$ and $x, y \in K$. Hence $x - y \in I$ and $x - y \in K$. Thus $x - y \in I \cap K$. Let $a \in I \cap K$ and $r \in R$. Then $ra \in I$ and $ra \in K$. Hence $ra \in I \cap K$. Thus $I \cap K$ is an ideal of R.

By hypothesis, there is an $x \in I \setminus K$ and $y \in K \setminus I$. Assume $I \cup K$ is an ideal. Hence $x - y \in I \cup K$. Thus $x - y \in I$ or $x - y \in K$. If $x - y \in I$, then $y \in I$, a contradiction. If $x - y \in K$, then $x \in K$, a contradiction.

3) Let $I = span\{6\} = 6Z$ and $K = span\{15\} = 15Z$ (note I, K are ideals of Z). Then $I \cap K = nZ$ for some integer n. Find n.

Sketch: Note that $6 \mid n$ and $15 \mid n$. Hence $n = LCM[6, 15] = 30$

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

Hadeel Kittaneh
900093357

Homework 2

Question 1 :

i) ⇒ Let $I = I_1 \times I_2$ be prime, then $\frac{R}{I} \approx \frac{R_1}{I_1} \times \frac{R_2}{I_2}$.
$\frac{R}{I}$ is an integral domain as I is prime. Suppose I_1 and I_2 are both proper. Now "1" $\notin I_1$ and "1" $\notin I_2$.
let $a = (I_1, 1+I_2)$ and $b = (1+I_1, I_2)$ but $ab = (I_1, 1+I_1)(1+I_2, I_2)$
$= (I_1, I_2)$. So R/I contains zero divisors and hence not prime.
one of I_1 and I_2 must be the whole ring.

⇐ Let $R_1 \times I_2 = I$ where I_2 is a prime ideal of R_2. (w.l.o.g)
$\frac{R}{I} \approx \frac{R_1}{R_1} \times \frac{R_2}{I_2}$. Since $\frac{R_1}{R_1} \times \frac{R_2}{I_2}$ is an integral domain. So is $\frac{R}{I}$.
Hence, I is prime.

(ii) ⇒ let I be maximal then I is prime and by (i) $I = I_1 \times R_2$ or $I = R_1 \times I_2$ for some prime ideals I_1, I_2 of R_1, R_2 respectively.
Now, (w.l.o.g) let $I = I_1 \times R_2$.
$\frac{R}{I} \approx \frac{R_1}{I_1} \times \frac{R_2}{R_2}$. but R/I is a field since I is maximal. Hence I_1 must be a maximal ideal.

⇐ let $I_1 \times R_2 = I$ where I_1 is a maximal ideal of R_1 (w.l.o.g).
Then, $\frac{R_1}{I_1} \times \frac{R_2}{R_2}$ is a field. $\frac{R_1}{I_1} \times \frac{R_2}{R_2} \approx \frac{R}{I}$.
I must be maximal.

10

Question 2:

(i) Let $x \in R$ be irreducible of PID R. We show xR is maximal and and hence xR is Prime. Thus x is a prime of R.

Consider the ideal xR. By contradiction assume xR is not maximal, then $xR \subset I \subset R$ for some maximal proper ideal I.
Since R is a PID $\exists\, m \in R$ s.t. $I = mR$.
$x \in I$ so $x = mr$ for some $r \in R$, but x is irreducible so either m is a unit or r is a unit. m is not a unit as $m \in I$.
so $m = xr^{-1} \Rightarrow mR = xR$, which is a contradiction. Our initial assumption is wrong. xR is a maximal ideal

(ii) I is a prime ideal so $I \subseteq M$ for some maximal ideal M.
$\exists\, a \in R$ s.t. $I = aR$ where a is prime. $M = mR$ for some $m \in R$
$a \in M \Rightarrow a = mr$ for some $r \in R$, since a is prime $m \in I$ or $r \in I$.
- If $m \in I$, then $M = mR \subset I$ and Hence $M = I$ and we are done.
- If $r \in I$, then $\exists\, s \in R$ s.t. $r = as$, so $a = mr = mas$.

R is an integral domain, so cancellation laws hold. $\Rightarrow ms = 1$, which means m is a unit. Therefore $M = R$, so I is maximal.

10

Question 3:

Let I be a proper Prime ideal of R. Since I is Prime of R, R/I is an integral domain.
R is finite, so R/I is finite as well, but every finite integral domain is a field as proved in homework 1.
R/I is a field iff I is a maximal ideal of R. Hence, I is maximal.

5

Question 4:

char$(R) = p$ means $pr = 0 \ \forall\, r \in R$. Using the binomial theorem we get

$$(x+y)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} x^i y^{p^n - i} = x^{p^n} y^0 + \frac{p^n!}{(p^n-1)!} x^{p^n-1} y + \dots + \frac{p^n!}{(p^n-1)!\,(2p^n-1)!} x y^{p^n-1} + y^{p^n} x^0$$

p divides every term in the last expression except the first and the last so all terms vanish but not x^{p^n} and y^{p^n}. Hence,

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}$$

5

5

Question 5:

I and K being co-prime means $\exists\ i \in I$ and $k \in K$ such that $i + k = 1$.

$1 = 1^{m+n-1} = (i+k)^{m+n-1}$. using binomial theorem,

$$(i+k)^{m+n-1} = \sum_{j=1}^{m+n-1} \binom{m+n-1}{j} i^j k^{m+n-1}$$

$$= \underbrace{\sum_{j=1}^{n-1} \binom{m+n-1}{j} i^j k^{m+n-1-j}}_{(I)} + \underbrace{\sum_{j=n}^{m+n-1} \binom{m+n-1}{j} i^j k^{m+n-1-j}}_{(II)}$$

k^m is a factor of each term in (I) and $k^m \in K^m$.

i^n is a factor of each term in (II) and $i^n \in I^n$.

Thus the sum is in $I^n + K^m$ and hence $1 \in I^n + K^m$ which implies I^n and K^m are co-prime.

Question 6:

$I = x^2R$, $K = x^3R$. We show by contradiction

number 6

By staring, it is clear that x^5Q[x] = I (intersection) K . So if x^5Q[x] is a principal ideal of R, then I (intersection)K = x^5R.

0.5 x^5 is in I (Intersection) K, but 0.5x^5 is not in x^5R (since 1/2 is not in R)

Question 7:

5

R is a finite ring. Let $r_1, \dots, r_n$ be all non-zero elements of R. Take any $r \neq 0 \in R$, then $rr_1, \dots, rr_n$ are elements in R and are distinct since $rr_i = rr_j \Rightarrow rr_i - rr_j = 0 = r(r_i - r_j) \Rightarrow r_i - r_j = 0 \Rightarrow r_i = r_j$. for $1 \leq i, j \leq n$

Since $r \in R$ $rr_k = r$ for some $r_k \in R$ $r_k \neq 0$

Now take any arbitrary $a \in R$. $arr_k = ar \Rightarrow arr_k - ar = 0$

$\Rightarrow r(ar_k - a) = 0 \Rightarrow ar_k - a = 0 \Rightarrow ar_k = a$. r_k is a unit.

R is an integral domain and hence a field by problem 3 in homework 1.

MTH 532, HW III

Ayman Badawi

Submit by midnight Tuesday October 25, 2022, send pdf file only, easy to read and organized to abadawi@aus.edu

QUESTION 1. (Freshman dream): Let R be a commutative ring with $1 \neq 0$ such that $char(R) = p$ a prime number. Let $x, y \in R$. Prove that $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for every $n \geq 1$ [Hint: prove it directly or use math induction]

Proof. We use Math. Induction

i) Let $n = 1$. **Then** $(x+y)^p = x^p + pc_{p-1}x^{p-1}y + \cdots + pxy^{p-1} + y^p$ **(by the binomial expansion theorem, note that** $pc_{p-1} = pc_{p-2} = \cdots = p = 0$ **in** R**)**

ii) Assume that $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ **for some** $n \geq 1$

iii) We prove it for $n+1$. **Hence by (ii) and (i), we have**

$$(x+y)^{p^{n+1}} = \left((x+y)^{p^n}\right)^p = (x^{p^n} + y^{p^n})^p = x^{p^{n+1}} + y^{p^{n+1}}$$

QUESTION 2. Show that $Nil(R) \subseteq P$ for every prime ideal P of a commutative ring R.[Hint: not difficult, but important fact]

Proof. Let P **be a prime ideal of** R. **Let** $x \in Nil(R)$. **Hence** $x^n = 0 \in P$ **for some integer** $n \geq$. **Let** m **be the least positive integer such that** $x^m \in P$. **Thus** $x^{m-1}x \in P$. **Since** P **is prime, we have** $x^{m-1} \in P$ **or** $x \in P$. **Since** m **is the least positive integer such that** $x^m \in P$**, we conclude that** $x^{m-1} \notin P$. **Hence** $x \in P$.

QUESTION 3. (a)Let $K = Q(\sqrt{5}i) = \{a + b\sqrt{5}i \mid a, b \in Q\}$ $(i = \sqrt{-1})$. Prove that F is a field [: Hint it is straight forward to see that K is a commutative ring with 1, Do not show that. Just show that if $x = a + b\sqrt{5}i \in K^*$, then $x^{-1} \in K$. Note that then $x^{-1} = 1/x = \frac{a}{a^2+5b^2} - \frac{b\sqrt{5}i}{a^2+5b^2}$]

No comments, it is clear by the hint

(b) (nice) Let K as in (a) and $A = Q[x]$ prove that $\frac{A}{(x^2+5)A}$ is ring-isomorphic to K. [Hint : Construct a ring homomorphism from A ONTO K, then use the first isomorphism Theorem.]

Proof. Let $T : A \to K$ **such that** $T(f(x)) = f(\sqrt{5}i)$. **Let** $f_(x), f_2(x) \in A$. **Hence** $T(f_1(x) + f_2(x)) = f_1(\sqrt{5}i) + f_2(\sqrt{5}i) = T(f_1(x)) + T(f_2(x))$ **and** $T(f_1(x)f_2(x)) = f_1(\sqrt{5}i)f_2(\sqrt{5}i) = T(f_1(x))T(f_2(x))$. **Thus** T **is a ring homomorphism. We show that** T **is ONTO. Let** $y \in K$. **Then** $y = a + b\sqrt{5}i$ **for some** $a, b \in Q$. **Let** $f(x) = a + bx \in Q[x]$. **Then** $T(f(x)) = f(\sqrt{5}i) = a + b\sqrt{5}i = y$. **Hence T is ONTO. We know** $Ker(T) = \{h(x) \in A \mid T(h(x)) = h(\sqrt{5}i) = 0\}$ **is an ideal of** A. **Since** A **is a PID,** $Ker(T) = d(x)A$ **for some monic polynomial** $d(x)$ **such that** $T(d(x)) = d(\sqrt{5}i)) = 0$, **Since** $x^2 + 5$ **is the smallest such polynomial in** $Q[x]$. **We conclude that** $Ker(T) = (x^2+5)A$. **Thus we know** $A/Ker(T) \cong Range(T) = K$ **(since T is onto). Thus** $A/(x^2+5)A \cong K$.

(c)Let R be a PID. Prove that every prime ideal of R is maximal. [hint: Let I be a prime idea of R, then we know $I \subseteq M$ for some maximal ideal M of R. Show $M \subseteq I$, note that R is a PID]

Proof. Let P **be a prime ideal of** R. **Since** R **is a PID, we have** $P = pR$ **for some prime element** p **of** R. **Hence** $P = pR \subseteq M$ **for some maximal ideal** M **of** R. **Since** R **is a PID,** $M = yR$ **for some nonunit** y **of** R. **Thus** $p \in yR$. **Hence** $p = yw$ **for some** $w \in R$. **Since every prime element of an integral domain is irreducible and** $p = yw$**, we conclude** $w \in U(R)$. **Thus** $y = w^{-1}p$. **Hence** $y \in pR$. **Since** $y \in pR$ **and** $p \in yR$**, we conclude that** $P = M$ **is a maximal ideal of** R.

(d) Let R be a PID. Prove that every irreducible element in R is prime [use (c). Let x be irreducible, then xR lives inside a maximal ideal M of R. Note that, in general, for any ring R, if y in R is prime, then uy is prime for every u in U(R)]

Proof. Let x **be an irreducible element of** R. **Then** $xR \subseteq M$ **for some maximal ideal** M **of** R. **Since R is a PID and every maximal ideal of** R **is prime,** $M = pR$ **for some prime element** p **of** R. **Hence** $x = pw$ **for some** $w \in R$. **Since** x **is irreducible and** p **is not a unit of** R**, we conclude that** $w \in U(R)$. **Hence x is a prime element of** R,

FACTS (know), add to your common knowledge dictionary

Let R be a commutative ring with 1 and $f(x) \in R[x]$. Then

1) $f(x) \in Z(R[x])$ if and only if there is a $w \in Z(R)^*$ such that $wf(x) = 0$ [nice result, the proof is technical , you need to keep tracking of the coefficients of $f(x)$. So just know it]

2) $f(x) = a_n x^n + \cdots + a_1 x + b \in U(R[x])$ if and only if $a_1, ..., a_n \in Nil(R)$ and $b \in U(R)$[this is not hard to prove, it is easy to see that $a_n x^n + \cdots + a_1 x$ is a nilpotent and by HW 2 nilpotent + unit = unit]

QUESTION 4. Use the fact above

a) Convince me that $f(x) = 3x^5 + 2x + 4 \notin Z(Z_6[x])$ [Note $2, 3, 4 \in Z(Z_6)^*$]

By the FACT, There is no $a \in Z(R)^*$ **such that** $af(x) = 0$

b) Convince me that $f(x) = 10x^{2023} + 5x^3 + 10 \in Z(Z_{15}[x])$.

since $3f(x) = 0$**, by the FACT, we are done.**

c) Give me a polynomial of degree 1963, say $h(x)$, such that $h(x)(4x^9 + 2x + 6) = 0$ in $Z_{10}[x]$.

by (b)**, let** $f(x) = 3x^{1963} + 6x^{63} + 9$

d) Convince me that $f(x) = 6x^2 + 3x + 5 \notin U(Z_{12}[x])$

Since $3 \notin Nil(Z_{12})$**, by the FACT,** $f(x)$ **is not nilpotent.**

e) Convince me $2x^4 + 6x + 11 \in U(Z_{16}[x])$

Since $2, 6 \in Nil(Z_{16})$ **and** $11 \in U(Z_{16})$**, by the fact, we are done.**

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`

MTH 532, HW IV

Ayman Badawi

Submit by midnight Tuesday November 15, 2022, send pdf file only, easy to read and organized to abadawi@aus.edu

QUESTION 1. Let F be a finite field with p^n elements where $n \geq 2$. Prove that $(F, +)$ is never a cyclic group; note that some authors write $GF(p^n)$ (you read it, Galois field with p^n elements) to mean a finite field with p^n elements. [Hint: Note that F is a Z_p-module, use class notes]

Proof. By class notes F is a Z_p-module and $(F, +) \cong A = (Z_p, +)X \cdots \times (Z_p, +)$ ($n \geq 2$ times). By staring, each nonzero element in A is of order p (under addition mod p). Hence A has no elements of order p^n. Since $(F, +) \cong A$, F has no elements of order p^n. Thus $(F, +)$ is not cyclic.

Another proof. We know $char(F) = p$, i.e., $p.1_F = 1_F + \cdots + 1_F$ (p times) $= 0$. Let $a \in F^*$. Then $p.a = a + \cdots + a$ (p times) $= (p.1_F)a = 0.a = 0$. Thus the order of a under addition is p. Hence F has no elements of order p^n ($n \geq 2$). Hence $(F, +)$ is not cyclic.

QUESTION 2. (nice and applicable)

a) Let D be an integral domain and $f(x)$ be a monic polynomial of degree 2 or 3 in $D[x]$. Prove that $f(x))$ is irreducible in $D[x]$ if and only if there is no $a \in D$ such that $f(a) = 0$ (i.e., if and only if $f(x)$ has no roots in D)

Proof. Assume $f(x)$ is irreducible of degree n (degree 2 or 3 not needed for this direction), and $a \in D$. Then $f(x) \neq (x - a)h(x)$ for some $h(x) \in D[x]$, where $deg(h) < deg(f)$. Thus $f(a) \neq 0$ for every $a \in D$. For the converse, assume degree(f) = 2. Since $f(a) \neq 0$ for every $a \in D$, we conclude that for every $b, c \in D$, $f(x) \neq (x - b)(x - c)$. Hence $f(x)$ is irreducible. Assume degree(f) = 3. Since $f(a) \neq 0$ for every $a \in D$, we conclude that $f(x) \neq (x - a)h(x)$ for every $a \in D$, and $h(x) \in D[x]$, where $deg(h) = 2$. Hence $f(x)$ is irreducible.

Note that degree 2 or 3 is needed for the converse. For example, if $f(x)$ is of degree 4 and $f(a) \neq 0$ for every $a \in D$, then $f(x)$ need not be irreducible. It is possible that $f(x) = h_1(x)h_2(x)$, where h_1, h_2 are irreducible of degree 2.

b) Prove that $f(x) = x^3 + x^2 + 2x + 1$ is irreducible in $Z_3[x]$.

Since $deg(f) = 3$ and $f(a) \neq 0$ for every $a \in Z_3$, by (a) we conclude that $f(x)$ is irreducible.

c) Write $f(x) = x^{16} + 1$ as product of irreducible elements in $D = Z_2[x]$ [Hint: Make use of the freshman dream]

Since $char(D) = 2$, by the freshman dream result, $x^{16} + 1 = x^{2^4} + 1 = (x + 1)^{2^4} = (x + 1) \times \cdots \times (x + 1)$ (16 times).

QUESTION 3. Let $F = GF(5^{28})$ and $L = Aut_{Z_5}(F)$. Recall that if H is a subgroup of L, then we say H fixes the subfield E of F if for each element in H (read again, for EACH element in H), say $h(x) \in H$, we have $h(e) = e$ for each $e \in E$.

Write down all subgroups of L, and for each subgroup of L find the unique fixed subfield of F.

Let $D = \{1, 2, 4, 7, 14, 28\}$ be the set of all factors of 28. By class notes, for each $m \in D$, F has one and only one subfield E_m, where $|E_m| = 5^m$.

We know $|Aut_{Z_5}(F)| = 28$ and $(Aut_{Z_5}(F), o)$ is a cyclic group generated by $f_1 : F \to F$ such that $f_1(a) = a^5$.

(i) For $m = 1$, $Aut_{Z_5}(F) =< f_1 : F \to F, f_1(a) = a^5 >$ and it fixed the subfield Z_5, note $|Aut_{Z_5}(F)| = 28$.

(ii) For $m = 2$, $Aut_{E_2}(F) =< f_2 : F \to F, f_2(a) = a^{5^2} >$ and it fixed the subfield $E_2 = \{a \in F \mid a^{5^2} = a\}$, note $|Aut_{E_2}(F)| = 14$.

(iii) For $m = 4$, $Aut_{E_4}(F) =< f_4 : F \to F, f_4(a) = a^{5^4} >$ and it fixed the subfield $E_4 = \{a \in F \mid a^{5^4} = a\}$, note $|Aut_{E_4}(F)| = 7$

(iv) For $m = 7$, $Aut_{E_7}(F) =< f_7 : F \to F, f_7(a) = a^{5^7} >$ and it fixed the subfield $E_7 = \{a \in F \mid a^{5^7} = a\}$, note $|Aut_{E_7}(F)| = 4$

(v) For $m = 14$**,** $Aut_{E_{14}}(F) =< f_{14} : F \to F, f_{14}(a) = a^{5^{14}} >$ **and it fixed the subfield** $E_{14} = \{a \in F \mid a^{5^{14}} = a\}$**, note** $|Aut_{E_{14}}(F)| = 2$

(vi) For $m = 28$**,** $Aut_{E_{28}}(F) = Aut_F(F) =< f_{28} : F \to F, f_{28}(a) = a^{5^{28}} = a >$ **and it fixed the subfield** F**, note** $|Aut_{E_{28}}(F)| = 1$

QUESTION 4. Let R be a commutative ring with $1 \neq 0$ and $S = \{P | P\ is\ a\ prime\ ideal\ of R\}$. Prove that $Nil(R) = \sqrt{R}$; recall that $\sqrt{R} = \cap_{P \in S} P$ [Hint: We know that $Nil(R) \subseteq P$ for every $P \in S$ and use the result that we proved: If D is a multiplicatively closed set and I is a proper ideal of R such that $D \cap I = \emptyset$, then there is a prime ideal W of R such that $I \subseteq W$ and $W \cap D = \emptyset$]

Proof. Since $Nil(R) \subseteq P$ **for every prime ideal** P **of** R**, it is clear that** $Nil(R) \subseteq \sqrt{R} = \cap_{P \in S} P$**. We show that** $\cap_{P \in S} P \subseteq Nil(R)$**. Deny. Then there is an** $x \in \cap_{P \in S} P \setminus Nil(R)$**. Thus** $x^m \notin Nil(R)$ **for every integer** $m \geq 1$**.**

Thus $D = \{1, x, x^2, ..., x^m, \cdots\}$ **is a multiplicatively closed set of** R **such that** $D \cap Nil(R) = \emptyset$**. Hence, by class result, there is a prime ideal** W **of** R **such that** $Nil(R) \subseteq W$ **and** $W \cap D = \emptyset$**. Thus** $x^m \notin W$ **for every integer** $m \geq 1$**. In particular,** $x \notin W$**. Since** W **is a prime ideal of** R **and** $x \notin W$**, we conclude that** $x \notin \sqrt{R} = \cap_{P \in S} P$**, a contradiction. Thus** $\cap_{P \in S} P \subseteq Nil(R)$**. Hence** $\sqrt{R} = \cap_{P \in S} P = Nil(R)$**.**

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`