Math 111B HW3

Zih-Yu Hsieh

January 28, 2025

1

Question 1 *Let R be a finite commutative ring. Show that every element of R is either a zero-divisor or a unit.*

Pf:
Suppose R is a finite commutative ring, then for each element $a \in R$ there are two cases to consider:

First, suppose there exists nonzero element $b \in R$ with $ab = ba = 0$, then a is a zero-divisor.

Else, if for all nonzero element $b \in R$ satisfies $ab = ba \neq 0$, which also implies $a \neq 0$ (since $0 \cdot b = 0$ for all $b \in R$). Then, for all $n \in \mathbb{N}$, $a^n \neq 0$: For base case $n = 1$, $a^1 = a \neq 0$, and suppose for given $n \in \mathbb{N}$, it satisfies $a^n \neq 0$, then by assumption, $a \cdot a^n = a^{n+1} \neq 0$, which by the principle of mathematical induction, $a^n \neq 0$ for all positive integer n.

Now, consider $S = \{a^n \mid n \in \mathbb{N}\} \subseteq R$, since R is finite, the set S is also finite. Thus, there must exists $m, n \in \mathbb{N}$ (assume $m > n$) with $a^m = a^n$. Which, $a^{n+(m-n)} - a^n = 0$, or $a^n(a^{(m-n)} - 1) = 0$.

Notice that since a is not a zero-divisor, then $(a^{(m-n)} - 1) = 0$ (if it's nonzero, then $a^n(a^{(m-n)} - 1) \neq 0$). Thus, $a^{(m-n)} = 1$, which $a \cdot a^{(m-n-1)} = 1$, showing that $a^{(m-n-1)} = a^{-1}$, thus a is a unit.

So for finite commutative ring R, if an element is not a zero-divisor, it is a unit.

2

Question 2 *Let R be a ring. Prove or disprove that $Z(R[X]) = Z(R)[X]$.*

Pf:

We'll prove that $Z(R)[X] = Z(R[X])$. Notice that if R is commutative ($Z(R) = R$), then the polynomial ring $R[X]$ is also commutative ($Z(R[X]) = R[X]$). So, for commutative ring, $R[X] = Z(R)[X] = Z(R[X])$. So, the following proof is based on a non-commutative ring R.

$\subseteq$: For all polynomial $p \in Z(R)[X]$, there exists $p_0, p_1, ..., p_n \in Z(R)$, with $p = p_0 + p_1X + ... + p_nX^n$. Which, for all $q \in R[X]$, there exists $q_0, q_1, ..., q_m$, with $q = q_0 + q_1X + ... + q_mX^m$. Then, the multiplication is as follow:

$$pq = c_0 + c_1X + ... + c_{m+n}X^{m+n}, \quad c_k = \sum_{i,j,\ i+j=k} p_iq_j$$

$$qp = c'_0 + c'_1X + ... + c'_{m+n}X^{m+n}, \quad c'_k = \sum_{j,i,\ j+i=k} q_jp_i$$

Since all $p_i \in Z(R)$, they commute with all elements in R, thus $c_k = c'_k$ for all index k, hence $pq = qp$. So, $p \in Z(R[X])$, indicating that $Z(R)[X] \subseteq Z(R[X])$.

$\supseteq$: We'll prove by contradiction. Suppose $Z(R[X]) \not\subseteq Z(R)[X]$, then there exists $p \in Z(R[X])$, such that some coefficient is not from $Z(R)$. Let $m \in \mathbb{N}$ be the largest index with $p_m \notin Z(R)$, which there exists $q \in R$, with $p_mq \neq qp_m$.

Also, let $n \in \mathbb{N}$ be the largest power of p (which $n \geq m$), then p can be expressed as follow:

$$p = p_0 + p_1X + ... + p_mX^m + p_{m+1}X^{m+1} + ... + p_nX^n$$

Then, by the assumption that m is the largest index with $p_m \notin Z(R)$, which $p_{m+1}, ..., p_n \in Z(R)$. Thus, the polynomial $p_{m+1}X^{m+1} + ... + p_nX^n \in Z(R)[X] \subseteq Z(R[X])$. Because $Z(R[X])$ itself is a ring, then:

$$p - (p_{m+1}X^{m+1} + ... + p_nX^n) = (p_0 + p_1X + ... + p_mX^m) \in Z(R[X])$$

So, WLOG, we can assume m is the largest power of p (since we can subtract out all the powers larger than m).

However, consider the following two expressions, pq and qp:

$$pq = (p_0 + p_1X + ... + p_mX^m)q = p_0q + p_1qX + ... + p_mqX^m$$

$$qp = q(p_0 + p_1X + ... + p_mX^m) = qp_0 + qp_1X + ... + qp_mX^m$$

For pq, the degree m coefficient is p_mq, while for qp, the degree m coefficient is qp_m. Since $p_mq \neq qp_m$, then $pq \neq qp$. However, since $q \in R[X]$ while $p \in Z(R[X])$, $pq = qp$, so this is a contradiction.

Thus, the assumption is false, $Z(R[X]) \subseteq Z(R)[X]$.

With the above two statements, $Z(R)[X] = Z(R[X])$.

3

Question 3 *Let R be an integral domain. Prove that $(R[X])^\times = R^\times$.*

Pf:

Since $R \subseteq R[X]$, then for all $a \in R^\times$, $a^{-1} \in R^\times$, which $a, a^{-1} \in R[X]$ satisfy $aa^{-1} = a^{-1}a = 1$, indicating that $a \in (R[X])^\times$. So, $(R)^\times \subseteq (R[X])^\times$.

Now, we'll use contradiction to prove that if $p \in R[X]$ has an inverse, then $p \in R$: Suppose there exists a non-constant polynomial $p \in R[X]$ with an inverse, then there exists $q \in R[X]$, with $pq = qp = 1$.

Let $p = p_0 + p_1X + ... + p_nX^n$ (which $n > 0$, and $p_n \neq 0$), and $q = q_0 + q_1X + ... + q_mX^m$.

Then, we can use induction to prove that for all $k \in \{0, ..., m\}$, $q_{m-k} = 0$:

For base case $k = 0$, since pq has the coefficient of $(n+m)$ degree being p_nq_m, because $(n+m) > 0$, while 1 is a constant polynomial, then $(n+m)$ degree should have coefficient 0, or $p_nq_m = 0$; yet, since $p_n \neq 0$ by assumption, and R is an integral domain, then $q_m = q_{m-0} = 0$.

Now, suppose for given $k \in \{0, ..., m-1\}$, every integer $0 \leq n \leq k$ satisfies $q_{m-n} = 0$, then, q can be expressed as follow:

$$q = q_0 + q_1X + ... + q_{m-(k+1)}X^{m-(k+1)} + q_{m-k}X^{m-k} + ... + q_mX^m$$

$$= q_0 + q_1X + ... + q_{m-(k+1)}X^{m-(k+1)}$$

Which, pq has the coefficient of $(n + (m - (k + 1)))$ being $p_nq_{m-(k+1)}$, since $k \leq (m-1)$, the $(k+1) \leq m$, thus $(m-(k+1)) \geq 0$. So, since $n > 0$, $(n+(m-(k+1))) > 0$; however, since $pq = 1$ a constant polynomial, so the coefficient of degree $(n + (m - (k + 1))) > 0$ is in fact 0, showing that $p_nq_{m-(k+1)} = 0$. Again, since $p_n \neq 0$ by assumption, then $q_{m-(k+1)} = 0$.

So, by the Principle of Mathematical Induction, every $k \in \{0, ..., m\}$ satisfies $q_{m-k} = 0$, showing that all index $i \in \{0, ..., m\}$ has $q_i = 0$.

However, this implies $q = q_0 + q_1X + ... + q_mX^m = 0$, or $pq = 0$, which is a contradiction (since $pq = 1$ by assumption).

So, the assumption is false, there doesn't exist a non-constant polynomial $p \in R[X]$ with an inverse.

Thus, for all $p \in (R[X])^\times$, p is a constant polynomial, or $p \in R$.

Then, suppose $q \in R[X]$ is an inverse of p, based on the same logic, q has an inverse implies $q \in R$, thus $p, q \in R^\times$, showing that $(R[X])^\times \subseteq R^\times$.

With both statements above, $(R[X])^\times = R^\times$.

4

Question 4 *Let R be a commutative ring. Prove or disprove that $(R[X])^\times = R^\times$.*

Pf:

Consider $R = \mathbb{Z}_4$, then consider $(3 + 2X) \in \mathbb{Z}_4[X]$:

$$(3 + 2X)^2 = (3 + 2X)(3 + 2X) = 3 \cdot 3 + (3 \cdot 2 + 2 \cdot 3)X + 2 \cdot 2X^2$$

$$= (9 \mod 4) + (12 \mod 4)X + (4 \mod 4)X^2 = 1 + 0X + 0X^2 = 1$$

Which, since $(3 + 2X) \notin R$, then $(3 + 2X) \notin R^\times$; however, $(3 + 2X)$ has an inverse, namely itself, so $(3 + 2X) \in (R[X])^\times$.

Hence, $(R[X])^\times \neq R^\times$ in this case.

5 (Not done)

Question 5 *Prove or disprove that only ideals of $M_2(\mathbb{R})$ are (0) and $M_2(\mathbb{R})$.*

Pf:

Since (0) is automatically an Ideal, thus to find some nontrivial ideal $I \subseteq M_2(\mathbb{R})$, we'll assume $I \neq (0)$ (so there are nonzero elements). Which, let $A \in I$ be a nonzero element, it has some entriy being $a \neq 0$.

Then, notice that by multiplying $\frac{1}{a}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ to A, the nonzero entry a gets rescaled to 1, so WLOG, we can assume the nonzero entry is 1. (Note: because I is an ideal, then every matrix in $M_2(\mathbb{R})$ multiplied by any matrix in I stays in I).

Also, regardless of which entry 1 is in, we can always use permutation matrix to permute the entry with 1 to any other entry. (Note 2: Use z_1, z_2, z_3 to represent the remaining entries):

$$\begin{pmatrix}1 & z_1\\ z_2 & z_3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}z_1 & 1\\ z_3 & z_2\end{pmatrix}, \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}z_1 & 1\\ z_3 & z_2\end{pmatrix} = \begin{pmatrix}z_3 & z_2\\ z_1 & 1\end{pmatrix}$$

$$\begin{pmatrix}z_3 & z_2\\ z_1 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}z_2 & z_3\\ 1 & z_1\end{pmatrix}, \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}z_2 & z_3\\ 1 & z_1\end{pmatrix} = \begin{pmatrix}1 & z_1\\ z_2 & z_3\end{pmatrix}$$

So, by multiplying the permutation matrix on the left or right, we can permute the nonzero entry to any other entries, hence WLOG, we can assume for every entry, there exists some matrix with that entry being nonzero.

Now, we'll prove that all standard basis matrices of $M_2(\mathbb{R})$ are in I:

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & z_1\\ z_2 & z_3\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ z_2 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$$

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & z_1\\ z_2 & z_3\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & z_2\end{pmatrix} = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$$

$$\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & z_1\\ z_2 & z_3\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ z_2 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$$

$$\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & z_1\\ z_2 & z_3\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & z_2\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

Hence, I contains the standard basis of $M_2(\mathbb{R})$.

Then, for all matrix $B \in M_2(\mathbb{R})$, the following is true:

$$B = \begin{pmatrix}a & b\\ c & d\end{pmatrix} = a\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + b\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + c\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} + d\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

Which each individual component by definition of ideals lie in I, since the basis elements are all in I; also, since I is an abelian group under addition, then the sum also stays in the group. Hence, $B \in I$, showing that $M_2(\mathbb{R}) \subseteq I$, or $I = M_2(\mathbb{R})$.

So, given an ideal $I \neq (0)$, we have $I = M_2(\mathbb{R})$, hence the only ideal for $M_2(\mathbb{R})$ is (0) and itself.

6

Question 6 *Does there exist a field of order 6? Justify your answer.*

Pf:

There does not exist a field of order 6.

In general, given F a finite field, it's order must be a prime power (there must exists prime p and positive integer n, with $|R| = p^n$). Furthermore, $p = char(F)$.

We'll prove it by contradiction: Suppose there exists a finite field F, which the order is not a prime power.

Then, since F is finite, $char(F) \neq 0$, then since F is an integral domain, $order(1) = char(F) = p$ for some prime number p (which since F is a group under addition, p divides $|F|$).

However, since we assume $|F|$ is not a prime power, there exists some distinct prime $q \neq p$, with q divides $|F|$. Then, based on Cauchy's Theorem, since F is a finite abelian group with q divides $|F|$, there exists an element $a \in F$, with $order(a) = q$. Thus, the following is true:

$$\sum_{i=1}^{q} a = q \cdot a = 0$$

Similarly, because p is the characteristic of F, the following is also true:

$$\sum_{i=1}^{p} a = p \cdot a = 0$$

Hence, $q \cdot a = p \cdot q = 0$.

Yet, here is a contradiction:

First, if $q > p$ (or $(q - p) > 0$), then the above equation implies $(q - p) \cdot a = 0$, so $order(a) < (q - p) < q = order(a)$, which is a contradiction.

Else, if $p > q$ (or $(p - q) > 0$), then since $(p - q) \cdot a = 0$, then either $a = 0$ or $(p - q)$ is a multiple of the order of a, namly $q \mid (p - q)$. Yet, if $a = 0$, then $order(a) = 1 \neq q$ (since prime $q > 1$), which is a contradiction; also, because p, q are distinct primes, p is not a multiple of q, which $(p - q)$ is also not a multiple of q, which is again a contradiction.

So, regardless of the case, we'll eventually run into a contradiction, then given finite field F, its order must be a prime power.

Furthermore, since $char(F) = p = order(1)$, then p divides $|F|$, showing that $|F|$ is not only a prime power, but prime power of p, its characteristic.

No Field has Order 6:

Since $6 = 2 \cdot 3$, which 6 is not a prime power. Thus, there doesn't exists a field with order 6 (since all finite field must have order being a prime power, as proven above).

7

Question 7 *Determine the smallest subring of $\mathbb{Q}$ that contains $1/2$. That is, describe the subring of $\mathbb{Q}$ which contains $1/2$ and every subring of $\mathbb{Q}$ containing $1/2$ also contains S.*

Pf:
Consider the set $S = \{\frac{m}{2^n} \in \mathbb{Q} \mid n \in \mathbb{N},\ m \in \mathbb{Z}\}$.

S is a Subring:

(1) For all $\frac{m_1}{2^{n_1}}, \frac{m_2}{2^{n_2}} \in S$, the following are true:

$$\frac{m_1}{2^{n_1}} + \frac{m_2}{2^{n_2}} = \frac{m_1 2^{n_2} + m_2 2^{n_1}}{2^{n_1+n_2}}, \quad \frac{m_1}{2^{n_1}} \frac{m_2}{2^{n_2}} = \frac{m_1 m_2}{w^{n_1+n_2}}$$

Which, since m_1, m_2 are all integers while n_1, n_2 are natural numbers, then the numerators above are all integers, while the denominators are nonnegative integer powers of 2, thus the two elements belong to S, S is closed under associative addition and multiplication (which, both are commutative and distributive, inherited from $\mathbb{Q}$).

(2) Since $0 = \frac{0}{2^1}$ abd $1 = \frac{2}{2^1}$, then $0, 1 \in S$, so both the zero and unity element of $\mathbb{Q}$ are in S.

(3) Given any $\frac{m}{2^n} \in S$, the inverse $\frac{-m}{2^n} \in S$, thus the additive inverse also exists.

With the properties above, S is a subring of $\mathbb{Q}$: It is closed under commutative addition, has zero element and additive inverse for all element, thus S is an abelian group under addition. On the other hand, it's closed under multiplication and has unity element, thus S is a monoid under multiplication. With the distributive property, S is a subring that contains $\frac{1}{2}$.

Every Subring $R \subseteq \mathbb{Q}$ containing $\frac{1}{2}$ contains S:
Now, assume that $R \subseteq \mathbb{Q}$ is a subring containing $\frac{1}{2}$.
For all element $\frac{m}{2^n} \in S$ (with $m \in \mathbb{Z}$ and $n \in \mathbb{N}$), since $\frac{1}{2} \in R$, then its power $(\frac{1}{2})^n = \frac{1}{2^n} \in R$; furthermore, because $\frac{1}{2^n} \in R$, then its integer multiple (sum of multiple $\frac{1}{2^n}$) is also contained in R, thus $\frac{m}{2^n} \in R$.
Hence, we can conclude that $S \subseteq R$, showing that S is the smallest subring of $\mathbb{Q}$ containing $\frac{1}{2}$.

8

Question 8 *Suppose a commutative ring R satisfies $x^3 = x$ for all $x \in R$, what are the possible values of $char(R)$?*

Pf:

(Note: The original problem is not possible, since if $\mathbb{Z} \subseteq R$, then take $2 \in \mathbb{Z}$, $2^3 = 8 \neq 2$. THe above is the modified question).

Suppose commutative ring R satisfies $x^3 = x$ for all $x \in R$, then in particular, $(1+1)^3 = (1+1)$. So:

$$8 \cdot 1 = (1+1)^3 = (1+1) = 2 \cdot 1$$

Hence, $8 \cdot 1 = 2 \cdot 1$, or $6 \cdot 1 = 0$. This implies that $order(1) \leq 6$, and also $order(1)$ divides 6.

So, the possible orders are $1, 2, 3, 6$; yet, since $1 \neq 0$ by convention, the $order(1) \neq 1$, so the only possibilities are $2, 3, 6$.

Then, since $order(1)$ is finite, this implies $char(R) \neq 0$, and $char(R) = order(1)$. Thus, the possible characteristics are $2, 3, 6$.

Examples:

For $char(R) = 2$, consider $\mathbb{Z}_2$: since $0^3 = 0$ and $1^3 = 1$, the property is satisfied

For $char(R) = 3$, consider $\mathbb{Z}_3$: it satisfies $0^3 = 0$, $1^3 = 1$, and $2^3 = 8 = 2(\mod 3)$, thus the property is satisfied.

For $char(R) = 6$, consider $\mathbb{Z}_6$: it satisfies $0^3 = 0$, $1^3 = 1$, $2^3 = 8 = 2(\mod 6)$, $3^3 = 27 = 3(\mod 6)$, $4^3 = 64 = 4(\mod 6)$, and $5^3 = 125 = 5(\mod 6)$, hence the property is again satisfied.

9

Question 9 *Prove or Disprove there is an integral domain R of order 15.*

Pf:

There does not exist an integral domain R with order 15.

In class, we've proven that for a finite commutative ring R, R is an integral domain if and only if R itself is a field.

Thus, if we assume there exists an integral domain R with order 15, since R is a finite field, its order must be a prime power (proven in **Question 6**).

Yet, since $|R| = 15 = 3 \cdot 5$, it is not a prime power, which is a contradiction.

So, the assumption is false, there doesn't exist an integral domain with order 15.

10

Question 10 *Let R be an integral domain of characteristic $p > 0$. Let $A = \{x^p \mid x \in R\}$. Prove or disprove that A is a subring of R.*

Pf:

We'll prove that A is a subring of R. First, since R is an integral domain, the its characteristic $p > 0$ must be prime.

Before starting, let's prove a lemma:

Lemma 1 *For all prime p, the binomial coefficient $\binom{p}{k}$ is divisible by p for all integer k satisfying $0 < k < p$.*

Given that $\binom{p}{k}$ is an integer for all k satisfying $0 < k < p$, which it is written in the following form:

$$\binom{p}{k} = \frac{p(p-1)...(p-k)}{k!}, \quad k!\binom{p}{k} = p(p-1)...(p-k)$$

The above equation indicates that $k!\binom{p}{k}$ is divisible by p. Yet, since $k < p$, then $k! = 1 \cdot 2...(k-1)k$ is not divisible by p (since it is a product of numbers coprime to p). Then, in case for the numbe to be divisible by p, $\binom{p}{k}$ must be a multiple of p (or else if $\binom{p}{k}$) is also coprime to p, the product $k!\binom{p}{k}$ is also coprime to p, which is a contradiction). So, the lemma is true.

A is a Submonoid under Multiplication:

Given that R is an integral domain (which is commutative), for all $x, y \in R$, $x^p, y^p \in A$, which $x^p y^p = (xy)^p$ while $xy \in R$. Thus, $x^p y^p = (xy)^p \in A$, showing that A is closed under multiplication.

Furthermore, since $1^p = 1 \in A$, then the unity element is also in A, showing that A is a submonoid of R under multiplication.

A is a Subroup under Addition:

Given that $0^p = 0 \in A$, A contains the zero element.

For all $x \in R$, there are two cases for the additive inverse:

- If $p = 2$, then $x^2 \in R$ implies $x^2 + x^2 = 0$ (by the definition of characteristic), thus $x^2 = -x^2$, so $x^2 \in A$ has an additive inverse in A.
- Else if $p \neq 2$, then p is odd ($p = 2k + 1$ for some $k \in \mathbb{Z}$). Thus:

  $$(-x)^p = (-x)^{2k+1} = ((-x)^2)^k(-x) = (x^2)^k(-x) = -x^{2k}x = -x^{2k+1} = -x^p$$

  So, $x^p \in A$ while $-x^p \in A$, hence x^p has an additive inverse in A.

Now, the only problem remain is addition: To prove that A is closed under addition, consider arbitrary $x, y \in R$, and the expression $(x + y)^p$. Under any commutative ring, the Binomial Theorem is true:

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} + x^p$$

Notice that the binomial expansion is true because R is an integral domain, which is commutative.

Then, by **Lemma 1**, for $k \in \{1, ..., p-1\}$, since $\binom{p}{k}$ is a multiple of p, hence the expression $\binom{p}{k} x^k y^{p-k} = 0$ (since here $\binom{p}{k}$ is some integer multiple of the characteristic of R, namely p).

So, $(x + y)^p = y^p + x^p$. For all $x, y \in R$, $x^p, y^p \in A$ satisfies $x^p + y^p = (x + y)^p \in A$, thus A is closed under multiplication.

A is a Subring of R:

From the above proof, given that A is an abelian subgroup of R under addition, and it is also a submonoid of R under multiplication, with the distributive property inherited from R, we can conclude that A is in fact a subring of R.