Math 111B HW3

Zih-Yu Hsieh

January 26, 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).

Because Ideal is an abelian subgroup under addition, which

6 (Not done)

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

Pf:
There does not exist a field of order 6.

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

9

Question 9

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 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 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 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 $(x+y)^p$:

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

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 the integer multiple of $x^k y^{p-k}$ is some 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.