Math 111B HW5

Zih-Yu Hsieh

February 18, 2025

1

Question 1 *Let R be a commutative ring. Prove or disprove that every non-constant monic polynomial $f(X) \in R[X]$ of degree n has at most n zeros in R.*

Pf:

Here is a counterexample: Consider $R = \mathbb{Z}_6$, and $f(X) \in R[X]$ defined as $f(X) = X + X^2$.
$f(X)$ is a degree 2 monic polynomial, yet the following is true:

$$f(0) = 0 + 0^2 = 0$$

$$f(2) = 2 + 2^2 = 2 + 4 = 6 \equiv 0 \ (mod\ 6)$$

$$f(3) = 3 + 3^2 = 3 + 9 = 12 \equiv 0 \ (mod\ 6)$$

$$f(5) = 5 + 5^2 = 5 + 25 = 30 \equiv 0 \ (mod\ 6)$$

Hence, $0, 2, 3, 5 \in \mathbb{Z}_6$ are 4 distinct roots of $f(X)$, while it is only a degree 2 polynomial. Hence, for R being a commutative ring, it is still possible to find monic polynomial in $R[X]$ with more zeroes in R than its degree.

2

Question 2 *Determine if the polynomial $f(X) = 21X^2 + 2X - 8 \in \mathbb{Z}[X]$ is irreducible. If it is not irreducible, what are its factors?*

Pf:

Given $f(X)$ stated above. Notice the following:

$$(7X-4)(3X+2) = 7X(3X+2) - 4(3X+2) = (21X^2 + 14X) + (-12X - 8) = 21X^2 + 2X - 8 = f(X)$$

Also, since $\mathbb{Z}$ is an integral domain, then $(\mathbb{Z}[X])^\times = (\mathbb{Z})^\times$:

First, since $\mathbb{Z} \subseteq \mathbb{Z}[X]$, then it's clear that $(\mathbb{Z})^\times \subseteq (\mathbb{Z}[X])^\times$ (since if $a \in (\mathbb{Z})^\times$, $a^{-1} \in (\mathbb{Z})^\times$, hence since $a, a^{-1} \in \mathbb{Z}[X]$ and $aa^{-1} = a^{-1}a = 1$, then $a, a^{-1} \in (\mathbb{Z}[X])^\times$).

Then, suppose $f(X) \in (\mathbb{Z}[X])^\times$, there exists $g(X) \in (\mathbb{Z}[X])^\times$, with $f(X)g(X) = 1$. Yet, since $1 \neq 0$, then $f(X), g(X) \neq 0$; also, since $\mathbb{Z}$ is an integral domain, then:

$$0 = \deg(1) = \deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X))$$

Since $\deg(f(X)), \deg(g(X)) \geq 0$, then the only possibility is $\deg(f(X)) = \deg(g(X)) = 0$. Hence, both $f(X), g(X)$ are constant, hence $f(X), g(X) \in \mathbb{Z}$, while $f(X)g(X) = 1$, showing that $f(X), g(X) \in (\mathbb{Z})^\times$. Therefore, $(\mathbb{Z}[X])^\times \subseteq (\mathbb{Z})^\times$.

The above two statements show that $(\mathbb{Z}[X])^\times = (\mathbb{Z})^\times$, then since $(7X-4), (3X+2) \notin \mathbb{Z}$, then $(7X-4), (3X+2) \notin (\mathbb{Z})^\times = (\mathbb{Z}[X])^\times$.

Because $f(X) = 21X^2 + 2X - 8 = (7X-4)(3X+2)$, while the two factors are not invertible, then $f(X)$ is reducible.

3

Question 3 *Find the quotient and remainder for the division of* $f(X) = 3X^4 + X^3 + 2X^2 + 1$ *by* $g(X) = X^2 + 4X + 2$ *in* $\mathbb{Z}_5[X]$.

Pf:

Notice that since the base field is $\mathbb{Z}_5$, we'll directly convert the coefficients without the modulo symbol. We'll do the division recursively:

First, consider $3X^2 \cdot g(X) = 3X^2(X^2 + 4X + 2) = 3X^4 + 12X^3 + 6X^2 = 3X^4 + 2X^3 + X^2$. Which:

$$f(X) - 3X^2 \cdot g(X) = (3X^4 + X^3 + 2X^2 + 1) - (3X^4 + 2X^3 + X^2) = -X^3 + X^2 + 1 = 4X^3 + X^2 + 1$$

So, $f(X) = 3X^2 \cdot g(X) + (4X^3 + X^2 + 1)$.

Then, consider $4X \cdot g(X) = 4X(X^2 + 4X + 2) = 4X^3 + 16X^2 + 8X = 4X^3 + X^2 + 3X$. Which:

$$(4X^3 + X^2 + 1) - 4X \cdot g(X) = (4X^3 + X^2 + 1) - (4X^3 + X^2 + 3X) = -3X + 1 = 2X + 1$$

So, $(4X^3 + X^2 + 1) = 4X \cdot g(X) + (2X + 1)$. Plug into the previous equation:

$$f(X) = 3X^2 \cdot g(X) + (4X^3 + X^2 + 1) = 3X^2 \cdot g(X) + 4X \cdot g(X) + (2X + 1) = (3X^2 + 4X)g(X) + (2X + 1)$$

Since $(2X + 1)$ has degree 1, which is less than 2 the degree of $g(X)$, hence the division process ends here.

Which, let $q(X) = (3X^2 + 4X)$ and $r(X) = (2X + 1)$, then $f(X) = q(X)g(X) + r(X)$, with $1 = \deg(r(X)) < \deg(g(X)) = 2$.

The division of $f(X)$ by $g(X)$ has the quotient $q(X) = 3X^2 + 4X$, and remainder $r(X) = 2X + 1$.

4

Question 4 *Find all zeros of the polynomial* $f(X) = X^{25} - 1 \in \mathbb{Z}_{37}[X]$.

Pf:

First, notice that since 37 is a prime, then the base ring $\mathbb{Z}_{37}$ is in fact a field. Hence, every element except for 0 is invertible, showing that $(\mathbb{Z}_{37})^\times = \mathbb{Z}_{37} \setminus \{0\}$. Then, since $|\mathbb{Z}_{37}| = 37$, we have $|(\mathbb{Z}_{37})^\times| = |\mathbb{Z}_{37} \setminus \{0\}| = 37 - 1 = 36$.

First, notice that $1 \in \mathbb{Z}_{37}$ satisfies $f(1) = 1^25 - 1 = 1 - 1 = 0$, hence 1 is a zero of $f(X)$.

Then, suppose $a \in \mathbb{Z}_{37}$ is a zero of $f(X) = X^{25} - 1$, which $f(a) = a^{25} - 1 = 0$, showing that $a^{25} = 1$.
Since $a \cdot a^{24} = a^{24} \cdot a = 1$, then a is invertible, hence $a \in (\mathbb{Z}_{37})^\times$.
Because $(\mathbb{Z}_{37})^\times$ is a group under multiplication, while $|(\mathbb{Z}_{37})^\times| = 36$, then $\mathit{order}(a) \;\Big|\; 36$, dividing the order of the group.
Similarly, since $a^{25} = 1$, then $\mathit{order}(a) \;\Big|\, 25$ (since the power of 25 returns to the identity of the group).
Hence, $\mathit{order}(a)$ must be a common factor of $25 = 5^2$ and $36 = 2^2 \cdot 3^2$, which $\mathit{order}(a) \;\Big|\; \gcd(25, 36) = 1$.

So, the only possibility is $\mathit{order}(a) = 1$, showing that $a^1 = a = 1$.
Therefore, the only zero for $f(X) = X^{25} - 1$ in $\mathbb{Z}_{37}$ is $X = 1$.

5

Question 5 *Find the quotient and remainder for the division of* $f(X) = 3X^5 + 5X^3 + X + 1$ *by* $g(X) = X^2 + 2X + 1$ *in* $\mathbb{Z}_7[X]$.

Pf:

Notice that the base field is $\mathbb{Z}_7$, we'll again convert the coefficients without the modulo symbol. We'll again do the division recursively:

First, consider $3X^3 \cdot g(X) = 3X^3(X^2 + 2X + 1) = 3X^5 + 6X^4 + 3X^3$. Which:

$$f(X) - 3X^3 \cdot g(X) = (3X^5 + 5X^3 + X + 1) - (3X^5 + 6X^4 + 3X^3) = -6X^4 + 2X^3 + X + 1 = X^4 + 2X^3 + X + 1$$

Hence, $f(X) = 3X^3 \cdot g(X) + (X^4 + 2X^3 + X + 1)$.

Then, consider $X^2 \cdot g(X) = X^2(X^2 + 2X + 1) = X^4 + 2X^3 + X^2$. Which:

$$(X^4 + 2X^3 + X + 1) - X^2 \cdot g(X) = (X^4 + 2X^3 + X + 1) - (X^4 + 2X^3 + X^2) = -X^2 + X + 1 = 6X^2 + X + 1$$

Hence, $(X^4 + 2X^3 + X + 1) = X^2 \cdot g(X) + (6X^2 + X + 1)$. Plug into the previous equation:

$$f(X) = 3X^3 \cdot g(X) + (X^4 + 2X^3 + X + 1) = 3X^3 \cdot g(X) + X^2 \cdot g(X) + (6X^2 + X + 1) = (3X^3 + X^2)g(X) + (6X^2 + X + 1)$$

Now, consider $6g(X) = 6X^2 + 12X + 6 = 6X^2 + 5X + 6$. Which:

$$(6X^2 + X + 1) - 6g(X) = (6X^2 + X + 1) - (6X^2 + 5X + 6) = -4X - 5 = 3X + 2$$

Hence, $(6X^2 + X + 1) = 6g(X) + (3X + 2)$. Plug into the previous equation:

$$f(X) = (3X^2+X^2)g(X)+(6X^2+X+1) = (3X^3+X^2)g(X)+6g(X)+(3X+2) = (3X^3+X^2+6)g(X)+(3X+2)$$

Since $(3X + 2)$ has degree 1, which is less than 2 the degree of $g(X)$, hence the division process ends here.

Which, let $q(X) = (3X^3 + X^2 + 6)$ and $r(X) = (3X + 2)$, then $f(X) = q(X)g(X) + r(X)$, while $1 = \deg(r(X)) < \deg(g(X)) = 2$. The division of $f(X)$ by $g(X)$ has the quotient $q(X) = 3X^3 + X^2 + 6$, and $r(X) = 3X + 2$.

6

Question 6 *Let p be a prime. prove or disprove that there exists a non-constant polynomial in $\mathbb{Z}_p[X]$ which has a multiplicative inverse.*

Pf:

Given p as a prime, we'll prove that there doesn't exist a non-constant polynomial in $\mathbb{Z}_p[X]$ that has a multiplicative inverse.

Since p is a prime, then the base ring $\mathbb{Z}_p$ is an integral domain.

Hence, suppose $f(X) \in \mathbb{Z}_p[X]$ has a multiplicative inverse $g(X) \in \mathbb{Z}_p[X]$, then $f(X)g(X) = 1$, showing that $f(X), g(X) \neq 0$ (or else $1 = 0$ is a contradiction).

Due to the property of integral domain, the following is true:

$$0 = \deg(1) = \deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X))$$

And, since $\deg(f(X)), \deg(g(X)) \geq 0$, then the only possibility is $\deg(f(X)) = \deg(g(X)) = 0$, showing that $f(X), g(X)$ are constants.

Hence, there doesn't exist a non-constant polynomial in $\mathbb{Z}_p[X]$ that has a multiplicative inverse, if p is prime.

7

Question 7 *Let k be a field and $R = k[X]$. Let $I = \{a_0 + a_1X + ... + a_nX^n \in R \mid \sum_{i=0}^n a_i = 0\}$. Show that I is an ideal of R. Is I principal? If yes, find a generator of I.*

Pf:

I is an ideal:

We'll first show that it is a subgroup under addition. Suppose $f(X), g(X) \in I$, which let $f(X) = a_0 + a_1X + ... + a_nX^n$, and $g(X) = b_0 + b_1X + ... + b_mX^m$. They satisfy $\sum_{i=0}^n a_i = 0 = \sum_{i=0}^m b_m$.

WLOG, assume that $n \geq m$. Then, $(f+g)(X)$ can be expressed as following:

$$(f+g)(X) = (a_0 + a_1X + ... + a_nX^n) + (b_0 + b_1X + ... + b_mX^m) = \sum_{i=0}^m (a_i + b_i)X^i + \sum_{j=m+1}^n a_jX^j$$

(Note: If $n = m$, then the second summation can be ignored).

Which, computing the sum of coefficients of $(f+g)(X)$, we get:

$$\sum_{i=0}^m (a_i + b_i) + \sum_{j=m+1}^n a_j = \left(\sum_{i=0}^m a_i + \sum_{j=m+1}^n a_j\right) + \sum_{i=0}^m b_i = \sum_{i=0}^n a_i + 0 = 0$$

Hence, $(f+g)(X) \in I$, showing that I is closed under addition.

Then, suppose $f(X) \in I$ (using the same expression as above). Which, $-f(X) = -(a_0 + a_1X + ... + a_nX^n) = -a_0 - a_1X - ... - a_nX^n$. Which, sum up the coefficients of $-f(X)$, it is as follow:

$$\sum_{i=0}^n -a_i = (-1)\sum_{i=0}^n a_i = 0$$

(Note: recall that $f(X) \in I$ implies that $\sum_{i=0}^n a_i = 0$).

Hence, $-f(X) \in I$, showing that every element in I has an additive inverse in I also.

Lastly, since $0 \in k[X]$ has all the coefficient being 0, the sum of coefficient is 0. Hence, $0 \in I$, showing that the zero element is in there.

Therefore, we can conclude that I is a subgroup under addition.

Then, to show that I is an ideal, it suffices to show that for all $f(X) \in I$, all $a \in k$, and all $l \in \mathbb{N}$, $aX^l \cdot f(X) \in I$.

Again, let $f(X) = a_0 + a_1X + ... + a_nX^n$, which $\sum_{i=0}^n a_i = 0$. Then, consider the following:

$$aX^l \cdot f(X) = a \cdot a_0X^l + a \cdot a_1X^{1+l} + ... + a \cdot a_nX^{n+l} = \sum_{i=0}^{l-1} 0 \cdot aX^i + \sum_{j=0}^n a \cdot a_jX^{j+l}$$

(Note: if $k = 0$, then the first summation term above can be ignored).

The sum of coefficient of $X^k \cdot f(X)$ is as follow:

$$\sum_{i=0}^{l-1} 0 + \sum_{j=0}^n a \cdot a_j = 0 + a\sum_{j=0}^n a_j = 0 + 0 = 0$$

Hence, given that $f(X) \in I$, every $a \in k$ and $l \in \mathbb{N}$ satisfies $aX^l \cdot f(X) \in I$.

Which, for all $g(X) \in k[X]$, $g(X) = b_0 + b_1X + ... + b_mX^m$ for some $b_0, b_1, ..., b_m \in k$. Hence, given $f(X) \in I$, $g(X) \cdot f(X)$ is as follow:

$$g(X) \cdot f(X) = b_0 f(X) + b_1 X \cdot f(X) + ... + b_m X^m \cdot f(X)$$

For all $l \in \{0, 1, ..., m\}$, since $b_l \in k$, then $b_l X^l \cdot f(X) \in I$; and since I is a subgroup under addition, then $g(X) \cdot f(X)$ is a sum of elements in I, which $g(X) \cdot f(X) \in I$.

Hence, we can conclude that I is in fact an ideal.

I is a Principal Ideal:

Recall that given a commutative ring R, $R[X]$ is a Principal Ideal Domain if and only if R is a field, hence since k is a field, $k[X]$ must be a Principal Ideal Domain. So, the ideal $I \subset k[X]$ is a principal ideal.

Generator of I:

Now, consider the polynomial $X - 1 \ \in k[X]$: Its sum of coefficients is given as $1 + (-1) = 0$, hence $X - 1 \ \in I$, implying that $(X - 1) \subseteq I$.

Also, for all $f(X) \in I$, let $f(X) = a_0 + a_1X + ... + a_nX^n$, which $\sum_{i=0}^n a_n = 0$. Then, consider the polynomial $g(X) \in k[X]$ defined as follow:

$$g(X) = -\sum_{i=0}^{n-1} \left(\sum_{j=0}^{i} a_j \right) X^i$$

Which, $(X - 1)g(X)$ is given as follow:

$$(X-1)g(X) = X \cdot g(X) - g(X) = -\sum_{i=0}^{n-1} \left(\sum_{j=0}^{i} a_j \right) X^{i+1} + \sum_{i=0}^{n-1} \left(\sum_{j=0}^{i} a_j \right) X^i$$

$$= -\left(\sum_{j=0}^{n-1} a_j \right) X^{(n-1)+1} - \sum_{i=0}^{n-2} \left(\sum_{j=0}^{i} a_j \right) X^{i+1} + \sum_{i=1}^{n-1} \left(\sum_{j=0}^{i} a_j \right) X^i + \left(\sum_{j=0}^{0} a_j \right) X^0$$

$$= \left(a_n - a_n - \sum_{j=0}^{n-1} a_j \right) X^n - \sum_{i=1}^{n-1} \left(\sum_{j=0}^{i-1} a_j \right) X^i + \sum_{i=1}^{n-1} \left(\sum_{j=0}^{i} a_j \right) X^i + a_0$$

$$= \left(a_n - \sum_{j=0}^{n} a_j \right) X^n + \sum_{i=1}^{n-1} \left(-\sum_{j=0}^{i-1} a_j + \sum_{j=0}^{i} a_j \right) X^i + a_0$$

$$= (a_n - 0)X^n + \sum_{i=1}^{n-1} a_i X^i + a_0$$

$$= \sum_{i=0}^{n} a_n X^n = f(X)$$

Hence, $f(X) = (X - 1)g(X)$, showing that $f(X) \in (X - 1)$, or $I \subseteq (X - 1)$.

With both containments being true, we can conclude that $I = (X - 1)$, hence $X - 1$ is a generator of I.