Math 111B HW6

Zih-Yu Hsieh

February 23, 2025

1

Question 1 *Let k be an infinite field and let $f(X), g(X) \in k[X]$ be such that a for all $a \in k^\times$. Prove or disprove that $f(X) = g(X)$.*

Pf:

We'll prove by contradiction, that $f(X) = g(X)$.

Suppose $f(X) \neq g(X)$, then $(f-g)(X) \neq 0$, hence $\deg(f-g) = n$ for some nonnegative integer n.

However, since k is a field, a nonzero polynomial over a field has at most n distinct zeroes, hence $(f-g)$ should have no more than n distinct zeroes.

Yet, since for the infinite field k, $k^\times$ is also infinite, and all $a \in k^\times$ satisfies $f(a) = g(a)$, or $(f-g)(a) = 0$, then a is a zero of $(f-g)$, showing that $(f-g)$ has infinite zeroes, which contradicts to the previous statement.

Hence, $f(X) = g(X)$ is enforced.

2

Question 2 *Let R be an integral domain such that the division algorithm holds in $R[X]$. Prove or disprove that R is a field.*

Pf:

Suppose R is an integral domain such that the division algorithm holds in $R[X]$. Then, for all nonzero element $a \in R$, consider X^2 and aX in $R[X]$:

Because division algorithm works, there exists unique pair of polynomials $q(X), r(X) \in R[X]$, with $X^2 = q(X) \cdot aX + r(X)$, such that $r(X) = 0$ or $\deg(r) < \deg(aX) = 1$.

Since $r(X) = 0$ or $0 \leq \deg(r) < 1$, then WLOG, can assume $r(X)$ is a constant, or $r(X) = \lambda \in R$. Hence, the above equation becomes:

$$X^2 = q(X) \cdot aX + \lambda, \quad X^2 - \lambda = q(X) \cdot aX$$

Because $X^2 - \lambda \neq 0$, then $q(X) \neq 0$; hencee, $2 = \deg(X^2) = \deg(q(X)) + \deg(aX) = \deg(q(X)) + 1$, showing that $\deg(q(X)) = 1$.

Hence, there exists $b, c \in R$ (with $b \neq 0$), such that $q(X) = bX + c$. So, the above equation becomes:

$$X^2 - \lambda = (bX + c)aX = abX^2 + acX$$

Because the two equations match up, then the leading coefficient also matches. Therefore, $1 = ab$, showing that a is invertible.

Because all nonzero element $a \in R$ is invertible, with the fact that R is an integral domain (which is commutative), R is a field.

3

Question 3 *Prove or disprove that* $f(X) = x^7 - X^5 + 2X^4 - 3X^2 - X + 2 \in \mathbb{Q}[X]$ *is irreducible.*

Pf:

Since $f(X)$ is a monic polynomial, then based on Rational Root Theorem, if there exists a rational root $q \in \mathbb{Q}$ of $f(X)$, not only if q is an integer, but also q divides the constant term of $f(X)$, namely 2.

So, consider the divisors of 2, the collection $\{\pm 1, \pm 2\}$:

Plug in $X = 1$, we get $f(1) = 1^7 - 1^5 + 2 \cdot 1^4 - 3 \cdot 1^2 - 1 + 2 = 1 - 1 + 2 - 3 - 1 + 2 = 0$, hence $1 \in \mathbb{Q}$ is a root of $f(X)$.

Then, using the division algorithm, with the linaer term $(X - 1)$, there exists unique polynomials $q(X), r(X) \in \mathbb{Q}[X]$, with $f(X) = (X-1)q(X) + r(X)$, and either $r(X) = 0$ or $0 \leq \deg(r) < \deg((X-1)) = 1$. Hence, $r(X)$ is in fact a constant.

Also, since $f(1) = (1-1)q(1) + r(1) = 0$, then $r(1) = 0$, showing that $r(X) = 0$. Hence, $f(X) = (X-1)q(X)$.

Finally, since $f(X) \neq 0$, then $q(X) \neq 0$; also, because $\deg(f) = 7$ and $\deg(f) = \deg((X-1)) + \deg(q) = 1 + \deg(q)$, then $\deg(q) = 6$, showing that q is a nonconstant polynomial in $\mathbb{Q}[X]$ (where $\mathbb{Q}$ is an Integral domain), hence nonconstant polynomials are not invertible.

Because $(X-1)$, $q(X)$ are both nonconstant polynomial, they're not invertible, hence $f(X)$ is a reducible element in $\mathbb{Q}[X]$.

4 (Potentially need to change)

Question 4 *Find all factors of $X^7 - X \in \mathbb{Z}_7[X]$.*

Pf:

Recall that Fermat's Little Theorem states that given any prime p, all $n \in \mathbb{N}$ satisfies $n^p \equiv n \ (mod\ p)$.

Then, for all $n \in \mathbb{Z}_7$, it is also true that $n^7 \equiv n \ (mod\ 7)$, showing that $n^7 - n \equiv 0 \ (mod\ 7)$. Hence, n is a zero of the equation $X^7 - X \in \mathbb{Z}_7[X]$, which since $\mathbb{Z}_7$ is a field (due to the fact that 7 is prime), $(X - n)$ is a factor of $X^7 - X$.

Also, since $\deg(X^7 - X) = 7$, then there are at most 7 zeroes (counting multiplicity) for this equation. Since all $n \in \mathbb{Z}_7$ is a zero, then each n has a multiplicity of 1, showing that $X^7 - X$ must be factored into distinct linear terms $(X - n)$.

Hence, $X^7 - X = X(X-1)(X-2)(X-3)(X-4)(X-5)(X-6)$, and arbitrary product of these distinct linear terms would be factor of $X^7 - X$.

5

Question 5 *Find a prime $p > 5$ such that $X^2 + 1 \in \mathbb{Z}_p[X]$ is irreducible.*

Pf:

Consider $p = 7$:

Recall that for a degree 2 or 3 polynomial in a polynomial ring $k[X]$ over a field k, it is reducible implies there is a zero in the field k. Hence,since $\mathbb{Z}_7$ is a field, to show that $X^2 - 1$ is irreducible in $\mathbb{Z}_7[X]$, it suffices to show that it has no zeroes in $\mathbb{Z}_7$.

Which, plug in all elements of $\mathbb{Z}_7$, we get:

$$0^2 + 1 = 1, \quad 1^2 + 1 = 2, \quad 2^2 + 1 = 5, \quad 3^2 + 1 = 10 \equiv 3 \ (mod\ 7)$$

$$4^2 + 1 = 17 \equiv 3 \ (mod\ 7), \quad 5^2 + 1 = 26 \equiv 5 \ (mod\ 7), \quad 6^2 + 1 = 37 \equiv 2 \ (mod\ 7)$$

Hence, $X^2 + 1$ has no zeroes in $\mathbb{Z}_7$, showing that $X^2 + 1$ is irreducible in $\mathbb{Z}_7[X]$.

6

Question 6 *Let* $f(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + a_nX^n \in k[X]$, *where* k *is a field and* $a_0 \neq 0$. *Let* $g(X) = a_n + a_{n-1}X + ... + a_1X^{n-1} + a_0X^n$. *Suppose that* $f(X)$ *has a linear factor in* $k[X]$. *Prove or disprove that* $g(X)$ *has a linear factor in* $k[X]$.

Pf:

First, since $f(X)$ has a linear factor, then there exists $a \in k$, where $f(X) = (X - a)q(X)$ for some $q(X) \in k[X]$. Hence, $f(a) = (a - a)q(a) = 0$, showing that a is a zero of f.

Notice that since $f(0) = a_0$, where by assumption $a_0 \neq 0$, showing that 0 is not a zero of f, hence $a \neq 0$. Then, due to the fact that k is a field and $a \neq 0$, then $a^{-1} \in k$ exists.

Now, consider $g(a^{-1})$:

$$g(a^{-1}) = a_n + a_{n-1}a^{-1} + ... + a_1(a^{-1})^{n-1} + a_0(a^{-1})^n = \sum_{i=0}^{n} a_{n-i}(a^{-1})^i$$

Which, multiply by a^n on both sides, we get:

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

(Note: the second line is the change of index $j = n - i$).

Which, the final expression is the same as $f(a)$, which is 0. Hence, $g(a^{-1}) = f(a) = 0$, showing that a^{-1} is a zero of g.

Then, because it is a root, we can always factor out the term $(X - a^{-1})$ as a linear term of $g(X)$. Hence, $g(X)$ has a linear factor in $k[X]$.

7

Question 7 *Prove or disprove that* $f(X) = X^3 + 4X^2 + X - 1 \in \mathbb{Q}[X]$ *is irreducible.*

Pf:

Notice that f is a degree 3 polynomial. Because $\mathbb{Q}$ is a field, then a degree 3 polynomial is reducible implies there is a zero in the field. Hence, if there is no zeroes in $\mathbb{Q}$, it implies that the polynomial f is irreducible.

Now, by Rational Root Theorem, because f is a monic polynomial, if $q \in \mathbb{Q}$ is a root of f, not only q is an integer, and q divides the constant coefficient, namely -1.

Hence, the only possible rational roots are ± 1. Yet, if plugin the values, we get:

$$f(1) = 1^3 + 4 \cdot 1^2 + 1 - 1 = 1 + 4 = 5, \quad f(-1) = (-1)^3 + 4 \cdot (-1)^2 + (-1) - 1 = -1 + 4 - 1 - 1 = 1$$

Because the only possible rational numbers are not the root of f, then f has no zeroes in $\mathbb{Q}$, showing that f is irreducible over $\mathbb{Q}$.

8

Question 8 *Let* $f(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + a_nX^n \in \mathbb{Z}[X]$. *Let* $x, y \in \mathbb{Z}$ *be such that* $(x, y) = 1$ *and* $f(x/y) = 0$ *when we consider* $f(X)$ *as a polynomial over* $\mathbb{Q}$. *Show that* $y \mid a_n$.

Pf:

If view f as a polynomial over $\mathbb{Q}$, then $f(x/y) = 0$ implies the following:

$$0 = f(x/y) = a_0 + a_1(x/y) + ... + a_{n-1}(x/y)^{n-1} + a_n(x/y)^n = \sum_{i=0}^{n} a_i(x/y)^i$$

Which, multiply both sides by y^n, we get:

$$0 = y^n \cdot 0 = y^n \cdot \sum_{i=0}^{n} a_i(x/y)^i = \sum_{i=0}^{n} a_i \cdot x^i \cdot y^{n-i} = a_nx^n + \sum_{i=0}^{n-1} a_i \cdot x^i \cdot y^{n-i}$$

$$-\sum_{i=0}^{n-1} a_i \cdot x^i \cdot y^{n-i} = a_nx^n, \quad -y \cdot \sum_{i=0}^{n-1} a_ix^i \cdot y^{n-i-1} = a_nx^n$$

(Note: for $0 \le i \le n-1$, $n - i - 1 \ge 0$, hence for the last equation we can factor out a y).

Since the left side is divisible by y, then the right side is also divisible by y; However, since x, y are coprime, then y cannot divide x, hence it cannot divide x^n. So, in case for a_nx^n to be divisible by y, y must divide a_n.