RINGS (MA 416) 2024-2025

Assignment 2

Due date: Wednesday October 30

Problems marked with $*$ are for submission. The rest are for independent study and discussion in the tutorials. Please submit solutions via the Canvas page, or in person at the lecture if you prefer paper.

1. For any nonzero polynomial $f(X)$ in $\mathbb{Z}[X]$, the *content* of $f(X)$ is defined as the greatest common divisor of all the coefficients of $f(X)$. For $f(X)$ and $g(X)$ in $\mathbb{Z}[X]$, show that the content of the product $f(X)g(X)$ is the product of the contents of $f(X)$ and $g(X)$.

2. Let $p \in \mathbb{Z}$ be a prime, and for any integer a let $[a]_p$ denote the congruence class of a modulo p. For $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, let $f_p(X)$ denote the polynomial

$$[a_n]_p + \cdots + [a_1]p + [a_0]_p \in \mathbb{Z}/p\mathbb{Z}[X].$$

   For example, if $p = 3$ and $f(X) = 5X^2 + 6X + 2$, then $f_3(X) = 2X^2 + 2$ in $\mathbb{Z}/3\mathbb{Z}[X]$.

   (a) Let $f(X)$ be a polynomial of degree at least 1 in $\mathbb{Z}[X]$, and assume that p does not divide the leading coefficient of $f(X)$.
      i. If $f(X)$ has a root in $\mathbb{Z}$, show that $f_p[X]$ has a root in $\mathbb{F}_p$ (where $\mathbb{F}_p$ denotes the field $\mathbb{Z}/p\mathbb{Z}$).
      ii. If $f(X)$ has a root in $\mathbb{Q}$, show that $f_p[X]$ has a root in $\mathbb{F}_p$.
      iii. * If $f(X)$ is reducible in $\mathbb{Q}[X]$, show that $f_p[X]$ is reducible in $\mathbb{F}_p[X]$
      iv. * If $f(X)$ is irreducible in $\mathbb{Q}[X]$, does it follow that $f_p[X]$ is irreducible in $\mathbb{F}_p[X]$?

   (b) * Why was the hypothesis that p does not divide the leading coefficent of $f(X)$ included in part (a)?

3. Use Question 2 to show that $2X^3 + X^2 - 4X - 1$ is irreducible in $\mathbb{Q}[X]$.

4. * Use Question 2 to show that $2X^3 + X^2 - 3X - 1$ is irreducible in $\mathbb{Q}[X]$.

5. Decide if each of the following polynomials is irreducible in the indicated ring :

   (a) $2x^2 - 5x + 5$ in $\mathbb{R}[x]$
   (b) * $2x^2 - 5x - 5$ in $\mathbb{R}[x]$
   (c) $x^3 - 5x^2 - 5x - 6$ in $\mathbb{Q}[x]$
   (d) * $x^3 + 2x^2 + 2x + 6$ in $\mathbb{Q}[x]$
   (e) $2x^5 - 6x^3 + 9x^2 - 15x + 12$ in $\mathbb{Q}[x]$

6. (a) Let $f(x)$ be a polynomial of degree ≥ 2 in $\mathbb{F}[x]$ for some field $\mathbb{F}$. Write $x = y + 1$ so that $f(x) = f(y+1) = g(y) \in \mathbb{F}[y]$. Show that $f(x)$ is irreducible in $\mathbb{F}[x]$ if and only if $g(y)$ is irreducible in $\mathbb{F}[y]$.

   (b) Show that the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$.

   (c) * For a prime $p \geq 3$, show that $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$.

7. The set of nth roots of unity in $\mathbb{C}$ is precisely the set of roots of the polynomial $x^n - 1$ in $\mathbb{C}[x]$.

   (a) Express each of the following polynomials as a product of irreducible factors in $\mathbb{Q}[x]$:
   $$x^4 - 1, \quad x^5 - 1, \quad x^6 - 1, \quad x^8 - 1.$$

   (b) An element ω of $\mathbb{C}$ is called a *primitive* nth root of unity if $\omega^n = 1$ but ω^k is not equal to 1 for any positive integer $k < n$. For example -1 is a fourth root of unity but it is not a primitive fourth root of unity, since $(-1)^2 = 1$; the primitive fourth roots of unity in $\mathbb{C}$ are i and $-i$.
   For $n = 4, 5, 6, 8$ identify a connection between the primitive kth roots of unity for each k dividing n and the irreducible factors in $\mathbb{Q}[x]$ of $x^n - 1$ found above.
   (Note: this meaning of "primitive" is not related to the one that we used for polynomials in $\mathbb{Z}[X]$, where it means that the gcd of the coefficients is 1.)

8. (a) Prove the following variant of the Eisenstein Irreducibility Criterion:
   Let $f(X) = a_n X^n + \cdots + a_1 X + a_0$ be a polynomial in $\mathbb{Z}[X]$, where $n \geq 1$ and $a_n \neq 0$. Suppose there is a prime p that divides all of $a_0, \ldots, a_{n-2}$, and suppose that p does not divide a_n and that p^2 does not divide a_0. Suppose further that $f(X)$ has no root in $\mathbb{Q}$. Then $f(X)$ is irreducible in $\mathbb{Q}[X]$.

   (b) * Prove the following variant of the Eisenstein Irreducibility Criterion:
   Let $f(X) = a_n X^n + \cdots + a_1 X + a_0$ be a polynomial in $\mathbb{Z}[X]$, where $n \geq 1$ and $a_n \neq 0$. Suppose p is a prime that divides a_0, and that p^2 does not divide a_0. Assume that p does not divide all the coefficients of $f(X)$, and let k be minimial with $p \not| a_k$. If $f(X)$ is reducible in $\mathbb{Q}[X]$, show that it has an irreducible factor of degree at most $n - k$.

9. Let R be a an integral domain (with at least two elements). Prove that R is a field if and only if the only ideals of R are R and $\{0_R\}$.

10. Which of the following are subrings of $\mathbb{Q}[x]$?

    (a) The set consisting of all polynomials of odd degree and the zero polynomial.

    (b) The set consisting of all polynomials of even degree and the zero polynomial.

    (c) The set consisting of all polynomials whose coefficients are all even integers.

    (d) The set consisting of all polynomials in which the coefficient of x^i is zero whenever i is odd.