MATH110BH Homework 5

Boran Erol

January 2024

1 Problem 1

Lemma 1.1. Let F be a field. Then, $F[X]$ has infinitely many irreducible polynomials.

Proof. This is the exact same proof as Euclid's proof that there are infinitely many prime numbers.

Suppose not. Let $f_1, ..., f_n$ be the irreducible polynomials. Consider $g = (f_1 \times f_2 \times ... \times f_n) + 1$. Since g is not irreducible, there's some f_i that divides g. Then, $f_i \mid 1$, which is a contradiction. $\square$

2 Problem 2

Lemma 2.1. $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i] \cong F_2$

Proof. First of all, notice that $(1+i)(1+i) = 2i$ and $(1+i)(1-i) = 2$, so $(1+i)R$ includes all Gaussian integers with even coefficients.

Consider the map $f : \mathbb{Z}[i] \to F_2$ defined by $a + bi \mapsto a + b \pmod 2$. This is clearly a group homomorphism.

Let's now prove that it is a ring homomorphism. Notice that $(a + bi)(c + di) = (ac - bd) + (ad + bc) = a(c + d) + b(c - d) = a(c + d) + b(c + d) = (a + b)(c + d)$, since $c + d = c - d$ in F_2. Thus, it's a ring homomorphism.

By the first isomorphism theorem, it suffices to prove that $ker(f) = (1 + i)R$.

Let $a + bi \in ker(f)$. There are two cases we need to handle:

1. Both a, b are even.

   Then, $a + bi \in (1 + i)R$ by the initial discussion.

2. Both a, b are odd. Then, $a + bi = 2k + 1 + 2mi + i$. Since $2k + 2mi \in (1 + i)R$, $a + bi \in (1 + i)R$.

   Now, let $a + bi \in (1 + i)R$. Then, $a + bi = (c + di)(1 + i) = c + ci + di - d$ for some $c, d \in \mathbb{Z}$. Notice that if c, d are both even or odd, both coefficients are even so $a + bi \in ker(f)$. If one of them is odd and the other is even, both coefficients are even so $a + bi \in ker(f)$.

$\square$

3 Problem 3

Lemma 3.1. Let $f \in \mathbb{Q}[x]$. $f \in \mathbb{Z}[x]$ if and only if $Cont(f) \in \mathbb{Z}$.

Proof. The forward implication is trivial. Let's prove the converse. Let $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Q}[x]$ and $m = min\{n : nf \in \mathbb{Z}[x]\}$. Then, $Cont(f) = \frac{1}{m} \gcd(ma_1, ..., ma_n)$. If $Cont(f) \in \mathbb{Z}$, the greatest common divisor is a multiple of m. Then, $\frac{ma_i}{m}$ is an integer for every i, so $f \in \mathbb{Z}[x]$. $\square$

Lemma 3.2. Let $f, g \in \mathbb{Q}[x]$ with $fg \in \mathbb{Z}[x]$. Then, $\exists a \in \mathbb{Q}^\times : af \in \mathbb{Z}[x] \wedge a^{-1}g \in \mathbb{Z}[x]$.

Proof. Let $Cont(f) = \frac{p_1}{q_1}$ and $Cont(g) = \frac{p_2}{q_2}$ be such that p_i and q_i are coprime. Since $fg \in \mathbb{Z}[x]$, $Cont(f)Cont(g) = Cont(fg) \in \mathbb{Z}$. Let $a = \frac{p_2}{q_2}$. Then, $Cont(af) \in \mathbb{Z}$ and $Cont(a^{-1}g) = 1$, so $af \in \mathbb{Z}[x]$ and $a^{-1}g \in \mathbb{Z}[x]$. We conclude the proof using the lemma above. $\square$

4 Problem 4

Let F be a field. Let R be the set of polynomials in $F[X]$ whose X-coefficient is 0. This set is clearly closed under addition and multiplication. $f = 1$ is also in R, so R is a subring of $F[X]$. Moreover, notice that X^2 and X^3 are irreducibles in R since $X \notin R$. Moreover, $X^6 = (X^2)^3 = (X^3)^2$ so X^6 has two different factorizations.

5 Problem 5

Constant polynomials aren't irreducible by definition. Both x and $x + 1$ are irreducible since every polynomial of degree 1 is irreducible. $x^2 + x + 1$ is the only polynomial of degree 2 without a root so it is irreducible. Similarly, $x^3 + x + 1$ and $x^3 + x^2 + 1$ are the only cubic polynomials without roots, so they're irreducible. As for fourth degree polynomials, notice that every polynomial should have the following form:

$$x^4 + ax^3 + bx^2 + cx + 1$$

since otherwise 0 is a root. Moreover, $a + b + c$ needs to be odd since otherwise 1 is a root. Since f shouldn't have roots, it also can't have a linear factor. Therefore, we only need to consider the square of irreducible polynomials of degree 2, of which there's one. Since $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, the irreducible polynomials are $x^4 + x^3 + 1$ and $x^4 + x + 1$.

6 Problem 6

Lemma 6.1. Let $f \in \mathbb{Z}[x]$ and $a, b \in \mathbb{Z}$. Then, $a - b \mid f(a) - f(b)$.

Proof. We'll induct on the degree of f. The statement is trivially true when $deg(f) = 0$ since every integer divides 0. Similarly, the statement is clearly true when $deg(f) = 1$ since $a - b \mid k(a - b)$. Now, assume the statement is true for some $n \in \mathbb{N}$. Let $f = a_{n+1}x^{n+1} + a_n x^n + ... + a_1 x + a_0$. Notice that $g = a_n x^n + ... + a_1 x + a_0$ is a polynomial of degree n. Also notice that

$$f(a) - f(b) = a_n(a^n - b^n) + (g(a) - g(b))$$

By the inductive hypothesis, $a - b \mid g(a) - g(b)$. Since $a - b \mid a^n - b^n$, $a - b \mid f(a) - f(b)$. $\square$

7 Problem 7

Since $\mathbb{Z}[X, Y] = \mathbb{Z}[X][Y]$, we can consider $y^n + (x^n - 1)$ as a polynomial with coefficients 1 and $(x^n - 1)$. Notice that $x - 1$ is an irreducible in $Z[X, Y]$. Since $\mathbb{Z}[X, Y]$ is a UFD, $x - 1$ is also a prime. Moreover, $x - 1 \mid x^n - 1$ and $x - 1 \nmid 1$. However, $(x - 1)^2 \nmid x^n - 1$. Then, by Eisenstein's Criterion, $y^n + (x^n - 1)$ is irreducible.

8 Problem 8

This is a special case of the rational root theorem. Let $f = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ and assume $a \in Q$ is a root of f. Let $a = \frac{p}{q}$ be the most simplified version of a. Then,

$$(\frac{p}{q})^n + a_{n-1}\frac{p}{q}^{n-1} + ... + a_1\frac{p}{q} + a_0 = 0$$

Multiplying by q^n and rearranging gives

$$-p^n = q(a_0 q^{n-1} + a_2 p q^{n-2} + ... + a_{n-1} p^{n-1})$$

Then, $q \mid p$. Since they're relatively prime, this produces $q = 1$.

9 Problem 9

Let $f = x^p - x$ be a polynomial in $(\mathbb{Z}/p\mathbb{Z})[x]$. By Fermat's Little Theorem, every non-zero value in $(\mathbb{Z}/p\mathbb{Z})$ is a root of f. Recall that every root produces a linear factor and that a polynomial has at most $deg(f)$ linear factors. Therefore, $f = x(x-1)(x-2)...(x-p+1)$.

10 Problem 10

Notice that $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$, so $x^4 + 4$ is not irreducible. There are two ways to see this:

First, notice that $x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - (2x)^2 = (x^2 + 2x + 2)(x^2 - 2x + 2)$.

Another, more straightforward way to see this is to consider the complex roots of x^4. Since all complex roots have integer coefficients, the product of conjugate pairs is going to be in $Z[x]$, so $x^4 + 4$ is reducible.