Math 110BH homework 5

Nathan Solomon

March 15, 2024

1

Show that over any field there exist infinitely many non-associate irreducible polynomials.

This is pretty much the same method we use to prove there are infinitely many prime numbers.

Let $\mathbb{F}$ be a field and suppose there is a finite set of all irreducible elements in $\mathbb{F}[x]$, excluding elements which are associate to an element in that set. Call that set $p = \{p_1, p_2, \ldots, p_n\}$. Note that p is nonempty, because it contains the irreducible polynomial $p_1 = x$.

Let $p_{n+1} = 1 + \prod_{i=1}^{n} p_i$. Then p_{n+1} is irreducible, since it is not divisible by any of the irreducible elements in p (and so p_{n+1} is also not associate to any of the other elements of p).

This is a contradiction, so there must be infinitely many non-associate irreducible elements in $\mathbb{F}[x]$.

2

Prove that the factor ring $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ is a field of two elements.

Let $\mathbb{F}_2$ be the field whose only elements are 0 and 1, and let $f : \mathbb{Z}[i] \to \mathbb{F}_2$ be the function defined by

$$f(a+bi) = \begin{cases} 0 & \text{if } a \text{ and } b \text{ have the same parity (both even or both odd)} \\ 1 & \text{if } a \text{ and } b \text{ have different parity (one even and one odd)} \end{cases}$$

for any integers a, b. Alternatively, we could define a parity function $p : \mathbb{Z} \to \mathbb{F}_2$ by $p(x) = \frac{1-(-1)^x)}{2}$, so then f can be defined by $f(a+bi) = p(a) + p(b)$.

For any Gauss integers $a+bi$ and $c+di$,

- $f(1) = 1$
- $f((a+bi)+(c+di)) = p(a) + p(c) + p(b) + p(d) = f(a+bi) + f(c+di)$.

- $f((a+bi)\cdot(c+di)) = f(ac-bd+(ad+bc)i) = p(ac)+p(bd)+p(ad)+p(bc) = (p(a+b))(p(c+d)) = f(a+bi)f(c+di)$.

Therefore f is a ring homomorphism, and f is clearly surjective.

For any element $a+bi \in \mathbb{Z}[i]$ for which $f(a+bi)=0$, $\frac{(a+bi)(1-i)}{2} = \frac{a-b-ai+bi}{2}$ is a Gauss integer, since $a-b$ and $b-a$ are even. Also, for any $(1+i)(a+bi) \in (1+i)\mathbb{Z}[i]$, $f((1+i)(a+bi)) = f(a-b+ai-bi) = p(a-b)+p(a-b) = 0$, so the kernel of f is $(a+i)\mathbb{Z}[i]$.

By the first isomorphism theorem (for rings),

$$\mathbb{Z}[i]/(1+i)\mathbb{Z}[i] \cong \mathbb{F}_2.$$

3

Let $f, g \in \mathbb{Q}[X]$ with $fg \in \mathbb{Z}[X]$. Prove that there is $a \in \mathbb{Q}^\times$ such that $af \in \mathbb{Z}[X]$ and $a^{-1}g \in \mathbb{Z}[X]$.

See the proof we did in class of Gauss' lemma.

4

Let F be a field. Prove that the set R of all polynomials in $F[X]$ whose X-coefficient is equal to 0 is a subring of $F[X]$ and that R is not a UFD. (Hint: Use $X^6 = (X^2)^3 = (X^3)^2$.)

The identity in R is the constant monic polynomial, which is the same as the identity in $F[x]$, and for any polynomials $a, b \in R$, $a+b$ and ab and $-a$ are also polynomials whose X-coefficient is 0. Therefore R is a subring of $F[x]$.

Next, we want to show that R is not a UFD, by showing that there are two distinct ways to write X^6 as a product of irreducible elements:

$$X^2 \cdot X^2 \cdot X^2 = X^6 = X^3 \cdot X^3.$$

In $F[x]$, if X^2 is written as a product of a and b, then either a and b both have degree 1, or one of them has degree 0. Similarly, if $ab = X^3$, then either one of them has degree 1 (and the other has degree two) or one of them has degree 0 (and the other has degree 3). That means if $a, b \in R$ and ab is either X^2 or X^3, then either a or b is a (nonzero) constant polynomial, which is a unit in R.

Since X^2 and X^3 are both irreducible, we have found distinct ways to write X^6, which is an element of R, as a product of irreducibles. Therefore R is not a UFD.

5

Find all irreducible polynomials of degree ≤ 4 in $(\mathbb{Z}/2\mathbb{Z})[X]$.

There are no irreducible polynomials of degree 0, and the only irreducible polynomials of degree 1 in $\mathbb{Z}/2\mathbb{Z}$ are x and $x+1$. In degree 2 or 3, a polynomial is irreducible if and only if it is not divisible by any degree 1 polynomial – the only such polynomials are x^2+x+1, x^3+x^2+1, and x^3+x+1. A polynomial of degree 4 is irreducible if and only if it is is not divisible by any degree 1 or 2 polynomial. There are 16 degree 4 polynomials we need to consider, but we can ignore the ones whose constant term is zero, because those are divisible by x. Going through the remaining 8 cases individually, we see that the the only degree 4 polynomials (in $\mathbb{Z}/2\mathbb{Z}$) are x^4+x+1, x^4+x^2+1, x^4+x^3+1, and $x^4+x^3+x^2+x+1$.

6

Let $f \in \mathbb{Z}[X], a, b \in \mathbb{Z}, a \neq b$. Prove that $a-b$ divides $f(a)-f(b)$. (Hint: $a-b$ divides a^n-b^n.)

Lemma 6.1. *$a-b$ divides a^n-b^n.*

Proof.

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}\right)$$

□

Let g be the function which is the same as f but without the highest order term. Then $f(a)-f(b)$ is equal to $g(a)-g(b)$ plus some multiple of a^n-b^n, so $a-b$ divides $f(a)-f(b)$ if and only if $a-b$ divides $g(a)-g(b)$. If f has degree zero, then it is clearly divisible by $a-b$, so by induction on the degree of f, $a-b$ must always divide $f(a)-f(b)$.

7

Prove that X^n+Y^n-1 is irreducible in $\mathbb{Z}[X,Y]$ for every $n>0$. (Hint: Use Eisenstein's Criterion.)

8

Let f be a monic polynomial in $\mathbb{Z}[X]$. Prove that if $a \in \mathbb{Q}$ is a root of f then $a \in \mathbb{Z}$.

Suppose a is a root of f which is rational but not an integer.

Then let $b, c \in \mathbb{Z}$ be nonzero coprime integers such that $\frac{b}{c} = a$ and c is not a unit. Also let n be the degree of f, and let $g = f - X^n$.

Since g is a degree $n-1$ polynomial with integer coefficients, $g(a)$ is the sum of terms which can all be written as fractions with denominator c^{n-1}, so

$$g(a) = \frac{\text{some integer}}{c^{n-1}}.$$

Because a is a root of f, $f(a) = \frac{b^n}{c^n} + g(a)$ has to be zero, which implies b^n is equal to some integer times $-c$. However, b^n and c^n are coprime, so b^n cannot be divisible by c. Since we have reached a contradiction, every root of a monic polynomial in $\mathbb{Z}[X]$ must either be an integer or be irrational.

9

Find all roots of $f = X^p - X$ in $(\mathbb{Z}/p\mathbb{Z})[X]$ (p prime) and factor f into a product of irreducible polynomials. (Hint: Use Fermat's Little Theorem.)

By Fermat's Little Theorem, if a is an integer and p is a prime integer, then $a^p - a \equiv 0 \pmod{p}$, so every $a \in \frac{Z}{p\mathbb{Z}}$ is a root of $X^p - p$. That means $X^p - X$ must be divisible by $X - a$ for every $a \in \frac{Z}{p\mathbb{Z}}$, so

$$X^p - X = X(X-1)(X-2)\cdots(X-(p-1)).$$

10

Determine whether $X^4 + 4$ is irreducible in $\mathbb{Z}[X]$.

This is reducible because

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

and $X^2 \pm 2X + 2$ is not a unit in $\mathbb{Z}[X]$.