Math 4108 HW3

Pengfei Zhu

January 24, 2024

1. Show that $\mathbb{Z}[X]$ is not a PID.

Proof. by contradiction.
Consider an example of ideal define as following:

$$\langle 2, X\rangle = \{2f(X) + Xg(X) : f(X), g(X) \in \mathbb{Z}[X]\},$$

consisting of all polynomials whose constant term is even. We will show that $\langle 2, X\rangle$ is not principal. We first notice that $\langle 2, X\rangle \neq \mathbb{Z}[X]$ because there are only even constant terms. For example, $1 \notin \langle 2, X\rangle$.

Now, suppose $\langle 2, X\rangle = \langle a(x)\rangle$ for some $a(x) \in \mathbb{Z}[X]$. Then we have $x = a(x)f(x)$ and $2 = a(x)g(x)$ for some $f(x), g(x) \in \mathbb{Z}[X]$ because $2 = 2 \cdot 1 + x \cdot 0 \in \langle 2, X\rangle$. However, the second equation implies that $a(x)$ must be a constant polynomial, that is $a(x) = \{\pm 2, \pm 1\}$.

Case 1: $a(x) = \pm 1$

$$\langle 2, X\rangle \ = \langle a(x)\rangle \ = (\pm 1) = \mathbb{Z}[X]$$

contradicting with the fact that $\langle 2, X\rangle \neq \mathbb{Z}[X]$

Case 2: $a(x) = \pm 2$

$$\langle 2, X\rangle \ = \langle a(x)\rangle \ = (\pm 2) = (2)$$

But then $x = \pm 2f(x)$, contradicting with the fact that $\pm 2f(x)$ has even coefficients. In either case, we get a contradiction. Thus, $\langle 2, X\rangle$ is not principal, and $\mathbb{Z}[X]$ is not a PID. □

2. Let K be a field. Show that K[X,Y] is not a PID.

wts: there is an ideal in $K[X, Y]$ that is not generated by a single element.

Consider the ideal $I = \langle X, Y\rangle$ in $K[X, Y]$, generated by X and Y. We want to show that I is not principal. Assume that I is a principal ideal, i.e., $I = \langle f\rangle$ for some $f \in K[X, Y]$.

Now, observe that X and Y are both in I, $f \mid x$ and $f \mid y$, so d must be a unit, and x and y are coprime. Therefore, $I = K[x, y]$. In particular, we have $1 \in I$.

Every element within I takes the form $px + qy$, where $p, q \in K[X, Y]$. This implies $1 = px + qy$ for certain $p, q \in K[X, Y]$. However, any element in the

form $px + qy$ does not have a nontrivial constant term, creating a contradiction. Consequently, I cannot be a principal ideal, establishing that $K[X, Y]$ is not a Principal Ideal Domain (PID).

3. Let F be any field with exactly four elements.

(a) Show that F has characteristic 2.

Suppose the characteristic of the field is 4. Then, in a field of characteristic 4, and it has properity that $1 + 1 \neq 0$. However, when computing $(1 + 1)(1 + 1)$ in this field:

$$(1 + 1)(1 + 1) = 1 + 1 + 1 + 1 = 0$$

This implies that 1+1 is a zero divisor, which is a contradiction. Therefore, the assumption that the characteristic is 4 leads to a contradiction. Hence, the characteristic must be 2.

(b) Show that both elements not in the prime subfield $\mathbb{Z}_2$ of F satisfy the polynomial equation $x^2 = x + 1$.

We define the field to be $F = 0, 1, a, b$ is a field. For multiplication, we consider 3 elements $1, a, b$ a cannot be 1 because then a^2 will also be 1. we can let $a^2 = b$, and then $a^3 = 1$ which works as a field. For addition, $a + b = 0 \implies a = -b = b$, since char$F = 2$. It also can't be a + b = a, a + b = b else b = 0 or a = 0. Thus, it must be $a + b = 1 \implies b = 1 - a = 1 + a$.

Now we have that for element a: $a^2 = a + 1$, and for element b: $b^2 = b + 1$ and $b = a^2$ which then satisfy the polynomial equation $b^2 = a + 1$.

(c) Show that F is isomorphic to $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$.

Consider a field F with four elements with characteristic to be 2. For any nonzero element a in F, the cubic polynomial $a^3 - 1$ can be factored as $(a - 1)(a^2 + a + 1) = 0$. This factorization holds true for all nonzero elements in F.

In the case where a belongs to F excluding the characteristic 2 elements ($a \in F \setminus \mathbb{Z}_2$), the expression $a^2 + a + 1$ equals zero, following from the factorization mentioned earlier. Furthermore, the polynomial $x^2 + x + 1$ is asserted to be irreducible over the field $\mathbb{Z}_2$. This means that it cannot be factored into linear polynomials over $\mathbb{Z}_2$. As a consequence of this irreducibility, it is asserted that for elements a in $F \setminus \mathbb{Z}_2$, the expression $a^2 + a + 1$ evaluates to zero. $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$. has the four elements {0,1,X,X+1}, which is the same field we found in part b with {0,1,a,b}. So F is isomorphic to $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$.

4. Let R be a commutative ring with unity, and f be a polynomial of degree $n \geq 1$ in $R[X]$.

(a) Prove that if R is an integral domain, then f has at most n roots in R.

From Howie's textbook, in Theorem 2.10, Let D be an integral domain, and let $D[X]$ be the polynomial ring of D. Then for all $p, q \in D[X]$, $\partial(pq) = \partial p + \partial q$. We can apply The Remainder Theorem and the Factor Theorem, if $a_1, \ldots, a_n$ are roots of f, then $f = (x - a_1) \ldots (x - a_n)g$ for some $g \in R[x]$, such that $\partial(f) = n + \partial(g)$ and $\partial(g) \geq 0$, hence $\partial(f) \geq n$. As a result, f has at most n roots in R.

(b) Give a concrete example to show that the statement above is false without the assumption that R is an integral domain.

$\mathbb{Z}/8\mathbb{Z}[x]$ is not an integral domain because R has zero divisors.

In $\mathbb{Z}/8\mathbb{Z}[x]$, consider the polynomials $g(x) = 2x$ and $h(x) = 4x$. Both $g(x)$ and $h(x)$ are nonzero polynomials, but their product is the zero polynomial:

$$g(x) \cdot h(x) = (2x) \cdot (4x) = 8x^2 \equiv 0 \pmod 8$$

This violates the integral domain property since we have two nonzero elements whose product is zero. Therefore, the proof in part (a) breaks down in this situation because the assumption of R being an integral domain is not satisfied for $\mathbb{Z}/8\mathbb{Z}[x]$.

5. Which of the following polynomials are irreducible over $\mathbb{Q}$?

(a) $x^3 + 2x^2 + 4x + 2$

To check irreducibility, we can use the Eisenstein's Criterion. In this case, Eisenstein's Criterion with the prime $p = 2$ is applicable. Since all coefficients except the leading coefficient are divisible by 2, and the constant term is not divisible by 2^2, the polynomial is irreducible over $\mathbb{Q}$.

(b) $x^3 + 2x^2 + 2x + 4$

It factors as $(x + 2)(x^2 + 2)$, so it is reducible over Q.

(c) $x^7 - 47$

This polynomial is irreducible over $\mathbb{Q}$ because it is a monic polynomial of prime degree.

(d) $x^4 + 15$

Use Eisenstein's criterion with $p = 3$. The conditions are satisfied since $f(x)$ is irreducible over $\mathbb{Q}$, with $3 \mid 15$, $3^2 \nmid 15$, and the rest of the coefficients are 0, so it is irreducible over Q.

6. Let p be any prime number.

a. Prove that $(x - 0) \cdot (x - 1) \cdot \ldots \cdot (x - (p - 1)) = x^p - x$ in $\mathbb{Z}_p[x]$.

Let's define the group $\mathbb{Z}_p^*$ of non-zero elements of $\mathbb{Z}_p$ is of order $p - 1$, and so $a^{p-1} = 1$ for all a in $\mathbb{Z}_p^*$. Then every element of $\mathbb{Z}_p$ is a root of

the polynomial $X^p - X$. Thus, by the Remainder Theorem, $X^p - X$ is divisible by $X(X-1)(X-2)\dots(X-(p-1))$. Because both left side and right side are monic and of degree p, so they are identical.

Above method uses Remainder and Factor Theorem, there is another method using Fermat's little theorem to show that $x^p - x$ is divisible by $(x-a)$ for all $a \in \mathbb{Z}_p$, which will lead to the same result.

b. Show that if two polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}_p[x]$ determine the same function on $\mathbb{Z}_p$, then $f(x) - g(x)$ is divisible by $x^p - x$.

Proof. Let $h(x) = f(x) - g(x)$. Since $f(x)$ and $g(x)$ determine the same function on $\mathbb{Z}_p$, we have $h(x) = 0$ for all $x \in \mathbb{Z}_p$.

By part (a), we know that $x^p - x$ is the zero polynomial in $\mathbb{Z}_p[x]$ when evaluated at any $x \in \mathbb{Z}_p$. Therefore, $h(x) \equiv 0 \pmod{p}$.

This implies that $h(x)$ is divisible by $x^p - x$ in $\mathbb{Z}_p[x]$. □

7. Find all monic irreducible quadratic (degree 2) polynomials over the field $\mathbb{Z}_5$.

Consider the polynomial $x^{25} - x$. $x^{p^n} - x$ is the product of irreducible polynomials in $\mathbb{F}_p[x]$ of degree d for all divisors of n, we focus on the irreducible polynomials over $\mathbb{F}_5$ of degrees 1 and 2.

The degree 1 irreducible polynomials are $x, x+1, \dots, x+4$. Factoring $x^{25}-x$ into irreducible polynomials, we isolate the degree 2 terms:

$$x^{25}-x = x(x^{24}-1) = x(x^{12}+1)(x^{12}-1) = x(x^{12}-4)(x^{12}-1) = x(x^6+2)(x^6-2)(x^6+1)(x^6-1)$$

Further simplifying, we find 10 number of degree 2 irreducible polynomials over $\mathbb{F}_5$, which are:

$$x^2-2, \quad x^2+2, \quad x^2+2x-1, \quad x^2-2x-1,$$
$$x^2+x+1, \quad x^2-x+1, \quad x^2+2x-2, \quad x^2-2x-2,$$
$$x^2+x-2, \quad x^2-x-2.$$

8. Find all monic irreducible cubic (degree 3) polynomials over the field $\mathbb{Z}_3$. Similar process as previous here, start with $x^{27}-x$, and we simplifying eventually get

$$x^3+2x^2+1, \quad x^3+2x^2+x+1, \quad x^3+2x+1, \quad x^3+x^2+2x+1,$$
$$x^3+x^2+2, \quad x^3+2x^3+x^2+x+2, \quad x^3+2x+2, \quad x^3+2x^2+2x+2.$$