MATH 417, HOMEWORK 10

CHARLES ANCEL

Chapter IV.22

Exercise 4. Find the sum and the product of the given polynomials in the given polynomial ring.

$$f(x) = 2x^3 + 4x^2 + 3x + 2, \ g(x) = 3x^4 + 2x + 4 \text{ in } \mathbb{Z}_5[x].$$

Proof. **For the Sum:** The sum $h(x)$ is found by adding the polynomials term by term:

$$\begin{aligned} h(x) &= f(x) + g(x) \\ &= (2x^3 + 4x^2 + 3x + 2) + (3x^4 + 2x + 4) \\ &= 3x^4 + 2x^3 + 4x^2 + 5x + 6. \end{aligned}$$

However, since we're in $\mathbb{Z}_5[x]$, we can reduce the coefficients modulo 5. This gives:

$$h(x) = 3x^4 + 2x^3 + 4x^2 + x.$$

For the Product: The product $p(x)$ is found by multiplying each term of $f(x)$ with each term of $g(x)$:

$$\begin{aligned} p(x) &= f(x)g(x) \\ &= (2x^3 + 4x^2 + 3x + 2)(3x^4 + 2x + 4) \\ &= 6x^7 + 12x^6 + 9x^5 + 10x^4 + 16x^3 + 22x^2 + 16x + 8. \end{aligned}$$

Again, we need to reduce the coefficients modulo 5 to get the polynomial in $\mathbb{Z}_5[x]$:

$$p(x) = x^7 + 2x^6 + 4x^5 + x^3 + 2x^2 + x + 3.$$

In conclusion, the sum and product in $\mathbb{Z}_5[x]$ are:

$$f(x) + g(x) = 3x^4 + 2x^3 + 4x^2 + x$$

$$f(x)g(x) = x^7 + 2x^6 + 4x^5 + x^3 + 2x^2 + x + 3.$$

□

The provided solution is well-structured and accurate.

Exercise 6. How many polynomials are there of degree ≤ 2 in $\mathbb{Z}_5[x]$? (Include 0.)

Proof. A polynomial of degree ≤ 2 in $\mathbb{Z}_5[x]$ has the general form:

$$ax^2 + bx + c$$

where a, b, and c are coefficients from $\mathbb{Z}_5$ and can take on any value from the set $\{0, 1, 2, 3, 4\}$.

1. For the coefficient a (which is the coefficient of x^2): Since we are considering polynomials up to and including degree 2, a can be 0 (for degree 0 or 1 polynomials) or any value between 1 and 4 (for degree 2 polynomials). Thus, there are 5 possibilities for a.

2. For the coefficient b (which is the coefficient of x): It can take on any value between 0 and 4, inclusive, regardless of the value of a. Thus, there are 5 possibilities for b.

3. For the constant term c: It can take on any value between 0 and 4, inclusive, regardless of the values of a and b. Thus, there are 5 possibilities for c.

Given these possibilities for each coefficient, the total number of polynomials of degree ≤ 2 is:

$$\text{Total polynomials} = 5 \times 5 \times 5 = 125.$$

Therefore, there are 125 polynomials of degree ≤ 2 in $\mathbb{Z}_5[x]$, which includes the polynomial 0. $\square$

Exercise 13. Find all zeros in the indicated finite field of the given polynomial with coefficients in that field. [Hint: One way is simply to try all candidates!]

$$x^3 + 2x + 2 \text{ in } \mathbb{Z}_7$$

Certainly! Let's provide a detailed breakdown of the computation in LaTeX format.

Proof. To find the zeros of $f(x)$ in $\mathbb{Z}_7$, we evaluate $f(x)$ for each element of $\mathbb{Z}_7$:

1. For $x = 0$:

$$f(0) = 0^3 + 2(0) + 2 = 2$$

2. For $x = 1$:

$$f(1) = 1^3 + 2(1) + 2 = 5$$

3. For $x = 2$:

$$f(2) = 2^3 + 2(2) + 2 = 16 \equiv 2 \pmod 7$$

However, since $2^3 = 8 \equiv 1 \pmod 7$, we have:

$$f(2) = 1 + 4 + 2 = 7 \equiv 0 \pmod 7$$

4. For $x = 3$:

$$f(3) = 3^3 + 2(3) + 2 = 35 \equiv 0 \pmod 7$$

5. For $x = 4$:

$$f(4) = 4^3 + 2(4) + 2 = 74 \equiv 4 \pmod 7$$

6. For $x = 5$:

$$f(5) = 5^3 + 2(5) + 2 = 135 \equiv 3 \pmod 7$$

7. For $x = 6$:

$$f(6) = 6^3 + 2(6) + 2 = 224 \equiv 6 \pmod 7$$

From the above computations, we see that $f(x)$ evaluates to zero in $\mathbb{Z}_7$ only for $x = 2$ and $x = 3$.

Thus, the zeros of $f(x)$ in $\mathbb{Z}_7$ are $x = 2$ and $x = 3$. □

Exercise 23. Mark each of the following true or false.

(a.) The polynomial $(a_n x^n + \cdots + a_1 x + a_0) \in R[x]$ is 0 if and only if $a_i = 0$, for $i = 0, 1, \cdots, n$.

(b.) If R is a commutative ring, then $R[x]$ is commutative.

(c.) If D is an integral domain, then $D[x]$ is an integral domain.

(d.) If R is a ring containing divisors of 0, then $R[x]$ has divisors of 0.

(e.) If R is a ring and $f(x)$ and $g(x)$ in $R[x]$ are of degrees 3 and 4, respectively, then $f(x)g(x)$ may be of degree 8 in $R[x]$.

(f.) If R is any ring and f (x) and g(x) in R[x] are of degrees 3 and 4, respectively, then $f(x)g(x)$ is always of degree 7.

(g.) If F is a subfield of E and $\alpha \in E$ is a zero of $f(x) \in F[x]$, then α is a zero of $h(x) = f(x)g(x)$ for all $g(x) \in F[x]$.

(h.) If F is a field, then the units in $F[x]$ are precisely the units in F.

(i.) If R is a ring, then x is never a divisor of 0 in $R[x]$.

(j.) If R is a ring, then the zero divisors in $R[x]$ are precisely the zero divisors in R.

Proof.
(a) The polynomial $(a_n x^n + \cdots + a_1 x + a_0) \in R[x]$ is 0 if and only if $a_i = 0$, for $i = 0, 1, \cdots, n$.
True. By definition of polynomial equality, two polynomials are equal if and only if their coefficients are equal.

(b) If R is a commutative ring, then $R[x]$ is commutative.
True. Polynomial multiplication is defined in terms of the ring multiplication, so if the coefficients from R commute, so will the polynomials in $R[x]$.

(c) If D is an integral domain, then $D[x]$ is an integral domain.
True. An integral domain is a commutative ring without zero divisors. If two non-zero polynomials in $D[x]$ are multiplied, the result will not be the zero polynomial, thus $D[x]$ has no zero divisors.

(d) If R is a ring containing divisors of 0, then $R[x]$ has divisors of 0.
True. If R has zero divisors, then so does $R[x]$ since the coefficients of the polynomials come from R.

(e) If R is a ring and $f(x)$ and $g(x)$ in $R[x]$ are of degrees 3 and 4, respectively, then $f(x)g(x)$ may be of degree 8 in $R[x]$.
False. The degree of the product of two polynomials is the sum of their degrees, so the degree of $f(x)g(x)$ will be $3+4=7$.

(f) If R is any ring and $f(x)$ and $g(x)$ in $R[x]$ are of degrees 3 and 4, respectively, then $f(x)g(x)$ is always of degree 7.
False. As discussed, there are cases where this might not be true, such as when the leading coefficient of one of the polynomials is a zero divisor in R.

(g) If F is a subfield of E and $\alpha \in E$ is a zero of $f(x) \in F[x]$, then α is a zero of $h(x) = f(x)g(x)$ for all $g(x) \in F[x]$.
True. If α is a zero of $f(x)$, then $f(\alpha) = 0$. Thus, $h(\alpha) = f(\alpha)g(\alpha) = 0 \times g(\alpha) = 0$.

(h) If F is a field, then the units in $F[x]$ are precisely the units in F.
True. In a polynomial ring, the only polynomials that have multiplicative inverses (and are thus units) are the non-zero constant polynomials, which correspond to the units in F.

(i) If R is a ring, then x is never a divisor of 0 in $R[x]$.
True. In any ring, no non-zero element can be a divisor of 0 unless the ring contains zero divisors. But x multiplied by any non-zero polynomial in $R[x]$ will not yield the zero polynomial.

(j) If R is a ring, then the zero divisors in $R[x]$ are precisely the zero divisors in R.
False. Consider $R = \mathbb{Z}_4$. In $R[x]$, the polynomial $2x$ is also a zero divisor since $2x \times 2x = 4x^2 = 0$, but $2x$ is not in R. So, $R[x]$ can have additional zero divisors not present in R. □

Exercise 25. Let D be an integral domain and x an indeterminate.

(a.) Describe the units in $D[x]$.

(b.) Find the units in $\mathbb{Z}[x]$.

(c.) Find the units in $\mathbb{Z}_7[x]$.

(a) Describe the units in $D[x]$.

Proof. The units in the polynomial ring $D[x]$ are precisely the units in D. This is because, in a polynomial ring over an integral domain, only the non-zero constant polynomials (those polynomials which are just constants from D with no terms involving x) have multiplicative inverses. Any polynomial with a term involving x (degree 1 or higher) cannot have a multiplicative inverse in $D[x]$ since its product with any other polynomial will always result in a polynomial of degree higher than 0, and thus cannot equal the multiplicative identity, which is 1. Therefore, the units in $D[x]$ are precisely the non-zero elements of D which are units. □

(b) Find the units in $\mathbb{Z}[x]$.

Proof. In $\mathbb{Z}$, the only units are 1 and -1 because they are the only integers that have multiplicative inverses in $\mathbb{Z}$. Specifically, $1 \times 1 = 1$ and $(-1) \times (-1) = 1$. Therefore, the only units in $\mathbb{Z}[x]$ are 1 and -1. □

(c) Find the units in $\mathbb{Z}_7[x]$.

Proof. In $\mathbb{Z}_7$, the units are the numbers that have multiplicative inverses modulo 7. These are all the numbers in $\mathbb{Z}_7$ except for 0, since $\mathbb{Z}_7$ is a field. Specifically, the units in $\mathbb{Z}_7$ are $\{1, 2, 3, 4, 5, 6\}$, and each of these numbers has a multiplicative inverse in $\mathbb{Z}_7$. For example, $3 \times 5 \equiv 1 \mod 7$, so 3 and 5 are multiplicative inverses of each other in $\mathbb{Z}_7$. Therefore, the units in $\mathbb{Z}_7[x]$ are $\{1, 2, 3, 4, 5, 6\}$. □

Exercise 27. Let F be a field of characteristic zero and let D be the formal polynomial differentiation map, so that:

$$D(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_1 + 2 \cdot a_2x + \cdots + n \cdot a_nX^{n-1}.$$

(a.) Show that $D : F[x] \to F[x]$ is a group homomorphism of $\langle F[x], +\rangle$ into itself. Is D a ring homomorphism?

(b.) Find the kernel of D.

(c.) Find the image of $F[x]$ under D.

(a) Show that $D : F[x] \to F[x]$ is a group homomorphism of $\langle F[x], +\rangle$ into itself. Is D a ring homomorphism?

Proof. For D to be a group homomorphism, it must satisfy the property:

$$D(f(x) + g(x)) = D(f(x)) + D(g(x))$$

for all $f(x), g(x) \in F[x]$.

Given $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$, where n and m are the degrees of $f(x)$ and $g(x)$ respectively, we differentiate:

$$\begin{aligned} D(f(x) + g(x)) &= D(a_0 + a_1x + \cdots + a_nx^n + b_0 + b_1x + \cdots + b_mx^m) \\ &= a_1 + 2a_2x + \cdots + na_nx^{n-1} + b_1 + 2b_2x + \cdots + mb_mx^{m-1} \\ &= D(f(x)) + D(g(x)) \end{aligned}$$

This shows that D is a group homomorphism with respect to addition.

However, D is not a ring homomorphism because it does not preserve multiplication. For example, consider two constant polynomials $f(x) = a$ and $g(x) = b$ in $F[x]$. We have:

$$D(f(x)g(x)) = D(ab) = 0$$

while

$$D(f(x))D(g(x)) = 0 \times 0 = 0$$

Although this example works, in general:

$$D(f(x)g(x)) \neq D(f(x))D(g(x))$$

For instance, take $f(x) = x$ and $g(x) = x$. Then:

$$D(f(x)g(x)) = D(x^2) = 2x$$

while

$$D(f(x))D(g(x)) = 1 \times 1 = 1$$

□

(b) Find the kernel of D.

Proof. The kernel of D consists of all polynomials $f(x)$ in $F[x]$ such that $D(f(x)) = 0$. From the definition of differentiation, it is clear that all constant polynomials will have a derivative of zero. Moreover, no other polynomial will have a derivative of zero since any polynomial with terms of degree 1 or higher will have a non-zero derivative.

Thus, the kernel of D is the set of all constant polynomials in $F[x]$. □

(c) Find the image of $F[x]$ under D.

Proof. The image of $F[x]$ under D is the set of all possible derivatives of polynomials in $F[x]$.

When differentiating a polynomial of degree n, we get a polynomial of degree $n-1$. Thus, the image of $F[x]$ under D will contain all polynomials of degree $n-1$ or less. However, since F has characteristic zero, even constant terms from the original polynomial (except the leading constant) will contribute to the derivative, ensuring that all possible coefficients in the field F can be achieved.

Therefore, the image of $F[x]$ under D is $F[x]$ itself, with the exception of the constant polynomials since a constant term in the original polynomial will vanish upon differentiation.

□

Chapter IV.23

Exercise 4. Find $q(x)$ and $r(x)$ as described by the division algorithm so that $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or of degree less than the degree of $g(x)$.

$$f(x) = x^4 + 5x^3 - 3x^2 \text{ and } g(x) = 5x^2 - x + 2 \text{ in } \mathbb{Z}_{11}[x].$$

Proof. Find $q(x)$ and $r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

where $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$.

Step 1: Normalize $g(x)$. Multiply $g(x)$ by the modular inverse of 5 in $\mathbb{Z}_{11}$, which is 9:

$$9 \cdot g(x) = 9 \cdot (5x^2 - x + 2) = x^2 - 9x + 7$$

Step 2: Perform Polynomial Long Division Now, perform the long division $\frac{f(x)}{g(x)}$:

$$\begin{array}{r|l}
9x^2 + 5x + 10 & x^4 + 5x^3 - 3x^2 \\
\hline
x^4 - 9x^3 + 7x^2 & \\
\hline
14x^3 - 10x^2 & \\
14x^3 - 126x^2 + 98x & \\
\hline
116x^2 + 98x & \\
116x^2 - 1044x + 812 & \\
\hline
1142x + 812 & \\
1142x - 10278 + 7990 & \\
\hline
10802 &
\end{array}$$

Reduce coefficients modulo 11:

$$116 \mod 11 = 6, \quad 1142 \mod 11 = 9, \quad 812 \mod 11 = 9, \quad 10802 \mod 11 = 2$$

So, the quotient is $q(x) = 9x^2 + 5x + 10$ and the remainder is $r(x) = 2$.

This satisfies the division algorithm conditions:

$$x^4 + 5x^3 - 3x^2 = (5x^2 - x + 2)(9x^2 + 5x + 10) + 2$$

in $\mathbb{Z}_{11}[x]$. □

Exercise 9. Find all generators of the cyclic multiplicative group of units of the given finite field. (Review Corollary 6.16.)

The polynomial $x^4 + 4$ can be factored into linear factors in $\mathbb{Z}_5[x]$. Find this factorization.

Proof. **Part 1: Factor the Polynomial** First, we note that in $\mathbb{Z}_5$, we can treat the number 4 as -1. Therefore,

$$x^4 + 4 \equiv x^4 - 1 \mod 5$$

This expression can be factored using the difference of squares:

$$x^4 - 1 = (x^2 + 1)(x^2 - 1)$$

Further factorizing $x^2 - 1$ as a difference of squares, and noting that $x^2 + 1$ can be expressed as $(x + 2)(x + 3)$ in $\mathbb{Z}_5[x]$:

$$x^4 - 1 = (x + 1)(x - 1)(x + 2)(x + 3) = (x + 1)(x + 4)(x + 2)(x + 3)$$

So, we have factored $x^4 + 4$ into linear factors in $\mathbb{Z}_5[x]$:

$$x^4 + 4 = (x + 1)(x + 2)(x + 3)(x + 4)$$

Part 2: Identify the Finite Field Since the polynomial $x^4 + 4$ can be factored into linear factors, the finite field defined by this polynomial is isomorphic to $\mathbb{Z}_5$, and its multiplicative group of units is $\mathbb{Z}_5^*$.

Part 3: Find the Generators The multiplicative group of units of a finite field of order p (where p is a prime) is cyclic of order $p - 1$. In this case, $\mathbb{Z}_5^*$ is of order 4. The generators of this group are the elements that are relatively prime to 5, which are $\{1, 2, 3, 4\}$. All of these elements are generators because $\mathbb{Z}_5^*$ is a cyclic group of order 4, and any element in a finite cyclic group of order n that is relatively prime to n is a generator.

Hence, all the elements $\{1, 2, 3, 4\}$ in $\mathbb{Z}_5^*$ are generators of the cyclic multiplicative group of units of the finite field defined by the polynomial $x^4 + 4$ in $\mathbb{Z}_5[x]$. □

Exercise 15. Show that $g(x) = x^2 + 6x + 12$ is irreducible over $\mathbb{Q}$. Is $g(x)$ irreducible over $\mathbb{R}$? Over $\mathbb{C}$?

Proof. **Part 1: Irreducibility over** $\mathbb{Q}$ To show that $g(x)$ is irreducible over $\mathbb{Q}$, we need to show that it cannot be factored into non-constant polynomials with coefficients in $\mathbb{Q}$.

The polynomial $g(x)$ is a quadratic polynomial, and it is well-known that a quadratic polynomial is irreducible over $\mathbb{Q}$ if and only if it has no roots in $\mathbb{Q}$.

Consider the discriminant of $g(x)$:

$$\Delta = b^2 - 4ac = (6)^2 - 4(1)(12) = 36 - 48 = -12$$

Since the discriminant is negative, there are no real roots, and hence no rational roots. Therefore, $g(x)$ is irreducible over $\mathbb{Q}$.

Part 2: Irreducibility over $\mathbb{R}$ Over the real numbers $\mathbb{R}$, a polynomial is irreducible if it is linear or a quadratic with no real roots. Since $g(x)$ is a quadratic polynomial with no real roots (as shown by the negative discriminant), it is irreducible over $\mathbb{R}$.

Part 3: Irreducibility over $\mathbb{C}$ Over the complex numbers $\mathbb{C}$, every non-constant polynomial can be factored into linear factors. Therefore, $g(x)$ is not irreducible over $\mathbb{C}$. In fact, we can find its roots using the quadratic formula:

$$x = \frac{-b \pm \sqrt{\Delta}}{2a} = \frac{-6 \pm \sqrt{-12}}{2} = \frac{-6 \pm 2i\sqrt{3}}{2} = -3 \pm i\sqrt{3}$$

So, $g(x)$ can be factored over $\mathbb{C}$ as:

$$g(x) = (x - (-3 + i\sqrt{3}))(x - (-3 - i\sqrt{3}))$$

□