Math 333 Problem Set 8
Solutions

Throughout this homework F denotes a field.

1. Let $D : \mathbb{R}[x] \to \mathbb{R}[x]$ be the derivative map. Is D a homomorphism of rings? An isomorphism? Be sure to justify your answer.

   This map is not a homomorphism, so it cannot be an isomorphism. For instance, we have $D(1 \cdot x) = D(x) = 1$ but $D(1)D(x) = 0 \cdot 1 = 0$.

2. Let $a, b \in F$ with $a \neq b$. Prove that $\gcd(x - a, x - b) = 1_F$ in $F[x]$.

   Proof. Let $d = \gcd(x-a, x-b) \in F[x]$. Note that d is necessarily monic and must be of degree 0 or 1 since it divides a polynomial of degree 1. If it is degree 0 we are done because the only monic polynomial of degree 1 is 1_F. Therefore, assume d has degree 1. Since d is monic, we have $d = x - c$ for some $c \in F$. Using the division algorithm we see that $x - a = (x - c) \cdot 1 + (c - a)$. Thus, $x - c \mid x - a$ if and only if $c = a$. The same arguments shows $x - c$ divides $x - b$ if and only if $c = b$. Since we are assuming $a \neq b$, this gives a contradiction. Thus, the degree of d must be 0. □

3. Modify the proof of the Euclidean algorithm we gave for $\mathbb{Z}$ to prove there is a Euclidean algorithm for $F[x]$. Use your algorithm to find the greatest common divisor of $f = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ and $g = 3x^3 + 5x^2 + 6x$ in $(\mathbb{Z}/7\mathbb{Z})[x]$. Express $\gcd(f, g)$ as a linear combination of f and g.

   Proof. We first show that if $f = gq + r$, then $\gcd(f, g) = \gcd(g, r)$. Let $d = \gcd(f, g)$ and $e = \gcd(g, r)$. Since $d \mid f$ and $d \mid g$ we have $d \mid r$ because $r = f - gq$. Thus, d is a common divisor of g and r so $d \mid e$. Conversely, we have $e \mid g$ and $e \mid r$, so $e \mid f$ as $f = gq + r$. Thus e is a common divisor of f and g so it divides d. Since d and e divide each other, we have $d = ue$ for some nonzero $u \in F$. However, since d and e are greatest common divisors they must be monic and so $u = 1_F$. Thus the claim is shown.

Now consider the following sequence:

$$\begin{aligned} f &= gq_1 + r_1 \quad \text{where } r_1 = 0_F \text{ or } \deg r_1 < \deg g \\ g &= r_1 q_2 + r_2 \quad \text{where } r_2 = 0_F \text{ or } \deg r_2 < \deg g \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \quad \text{where } r_n = 0_F \text{ or } \deg r_n < \deg r_{n-1} \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Observe that at each step one either gets a remainder of 0_F or the degree of the remainder strictly decreases. Since the collection of degrees of the remainders is a strictly decreasing sequence of positive integers it must eventually reach 1, in which case the next step must yield a remainder of 0_F. Now we apply the claim above to conclude that $\gcd(f, g) = \gcd(g, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0_F) = r_n$. □

For these particular polynomials we have if we set $f = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ and $g = 3x^3 + 5x^2 + 6x$, then:

$$\begin{aligned} f &= 6xg + r_1 \quad \text{where } r_1 = 5x^2 + 4x + 15 \\ g &= (2x+5)r_1 + r_2 \quad \text{where } r_2 = 4x + 3 \\ r_1 &= (3x+4)r_2 + 0. \end{aligned}$$

Thus, $\gcd(f, g) = r_2 = 4x + 3$. Using back substitution we see

$$\begin{aligned} r_2 &= g - (2x+5)r_1 \\ &= g + (5x+2)r_1 \\ &= g + (5x+2)(f - 6xg) \\ &= g + (5x+2)f - (30x+12)g \\ &= (5x+2)f + (5x+3)g. \end{aligned}$$

4. Prove that $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$.

Proof. Suppose that $f = x^2 + 1$ is reducible in $\mathbb{Q}[x]$, i.e., there are polynomials $g, h \in \mathbb{Q}[x]$ so that $f = gh$. Since we have $\deg(g) + \deg(h) = 2$ and any polynomial of degree 0 is a unit, it must be the case that g and h are linear. Write $g = cx + d$ and $h = sx + t$ for some $c, d, s, t \in \mathbb{Q}$. Observe that since $\deg(g) = \deg(h) = 1$ we must have c and s are nonzero. Thus, $x^2 + 1 = csx^2 + (ct + ds)x + dt$, i.e.,

$cs = 1$, $ct + ds = 0$, and $dt = 1$. Using that $s \neq 0$ we have $c = 1/s$. Moreover, since $dt = 1$ we have d and t are nonzero so we have $d = 1/t$. Substituting this we obtain $0 = ct+ds = (1/s)t+(1/t)s$, i.e., $t^2 = -s^2$. However, this is a contradiction as $t^2 > 0$ and $-s^2 < 0$. Thus, $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$. □

5. List all associates of $x^2 + x + 1$ in $(\mathbb{Z}/5\mathbb{Z})[x]$.

The units of $(\mathbb{Z}/5\mathbb{Z})[x]$ are $1, 2, 3, 4$ so the associates of $x^2 + x + 1$ are $x^2 + x + 1$, $2(x^2 + x + 1)$, $3(x^2 + x + 1)$, and $4(x^2 + x + 1)$.

6. Prove that $f \in F[x]$ is irreducible if and only if for every $g \in F[x]$, either $f \mid g$ or $\gcd(f, g) = 1_F$.

Proof. First suppose that f is irreducible and let $g \in F[x]$. Let $d = \gcd(f, g)$. Since f is irreducible the only divisors of f are units and associates. If d is a unit then it is 1_F since the only units in $F[x]$ are the nonzero elements of F and the only monic element of F is 1_F. If d is not a unit, then d is an associate of f, i.e., $d = uf$ for some nonzero $u \in F$. However, this gives $f \mid g$.

Now assume that for every $g \in F[x]$ we have either $f \mid g$ or $\gcd(f, g) = 1_F$. Suppose that $f = gh$ for some $g, h \in F[x]$. We have either $f \mid g$, which would give $f \mid g$ and $g \mid f$ so $f = gc$ for some nonzero $c \in F$. Thus, h is a unit and g is an associate of f. If $f \nmid g$, then $\gcd(f, g) = 1_F$ so there exists $s, t \in F[x]$ so that $fs + gt = 1_F$. This gives $1_F = ghs + gt = g(hs + t)$, i.e., g is a unit. Thus, in either case we see f can only be factored into a product of a unit and an associate so f is irreducible. □

7. Find a nonzero polynomial in $(\mathbb{Z}/3\mathbb{Z})[x]$ that induces the zero function on $\mathbb{Z}/3\mathbb{Z}$.

Define $f = x(x - 1)(x - 2)$. The leading coefficient of this is 1 so it is a nonzero polynomial. However, when we view this as a polynomial function it vanishes on each element of $\mathbb{Z}/3\mathbb{Z}$.

8. Use the factor theorem to show that $x^7 - x$ factors in $(\mathbb{Z}/7\mathbb{Z})[x]$ as $x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$ without doing any polynomial multiplication.

Proof. Observe that by direct computation one sees that each element of $\mathbb{Z}/7\mathbb{Z}$ is a root of $f = x^7 - x$. This shows that $x - j$ divides f for each $j \in \mathbb{Z}/7\mathbb{Z}$. We now apply problem 2 to deduce that $\gcd(x-a, x-b) = 1$ for each $a, b \in \mathbb{Z}/7\mathbb{Z}$ with $a \neq b$. It only remains to show that if $g, h \in F[x]$ with $\gcd(g,h) = 1_F$ and $g \mid k$ and $h \mid k$ for some $k \in F[x]$, then $gh \mid k$. Since $g \mid k$, there exists $s \in F[x]$ so that $k = gs$. Since $h \mid k$, we have $h \mid gs$. However, $\gcd(g,h) = 1_F$ so we must have $h \mid s$. This gives the result. $\square$

9. For what values of k is $x - 2$ a factor of $x^4 - 5x^3 + 5x^2 + 3x + k$ in $\mathbb{Q}[x]$.

We have that $x-2$ is a factor of $f = x^4 - 5x^3 + 5x^2 + 3x + k$ if and only if 2 is a root of the polynomial function induced on $\mathbb{Q}$ by f. Observe that $f(2) = 2 + k$. Thus, we require $k = -2$.

10. If f and g are associates in $F[x]$, show they have the same roots in F. If f and g have the same roots in F, are they necessarily associates? Be sure to justify your answer.

Let f and g be associates in $F[x]$, i.e., there exists a nonzero $u \in F$ so that $f = ug$. Let α be a root of f, i.e., $f(\alpha) = 0_F$ where $f(\alpha)$ denotes the value of the polynomial function at α. Since $f = ug$ as polynomials, this gives $f = ug$ as polynomial functions. Thus, $u(\alpha)g(\alpha) = ug(\alpha) = f(\alpha) = 0_F$ where we have used $u \in F$ so $u(\alpha) = u \neq 0_F$. Thus, $g(\alpha) = 0$ so α is a root of g. Conversely, if β is a root of g then $f(\beta) = ug(\beta) = 0_F$, so β is a root of f. Hence, if f and g are associate they have the same roots.

Let $f = x$ and $g = x^2$. These polynomials have the same roots, namely 0_F, but they are not associate as $g = xf$ and since $\deg(x) = 1$, x is not a unit.