# Intro to Modern Algebra: Homework #2

Due on November 2 at 9:30am

*Professor Lorenz 9:30-11:00*

**Sam Cook**

# Problem 6

Which of the following subsets of $\mathbb{R}[x]$ are subrings of $\mathbb{R}[x]$.

a All polynomials with constant term of $0_R$

b All polynomials of degree 2.

### Solution

**a)** This is a subring. We will show that it is a nonempty subset closed under subtraction and multiplication. First, zero is a polynomial with the constant term $0_R$, so it is a nonempty subset. Next, consider polynomials $a, b \epsilon \mathbb{R}[x]$. Then if we subtract them and $0_R$, we get $(a + 0_R) - (b + 0_R) = (a - b) + (0_R - 0_R) = a - b$, and since $a, b \epsilon R$, it is closed under subtraction. Similarly for multiplication, we get $(a + 0_R) * (b + 0_R) = (ab) + (0_R * b) + (0_R * a) + 0_R = ab$, so it is similarly closed under multiplication. Therefore, it is a subring of $\mathbb{R}[x]$.

**b)** This is not a subring because it is not closed under multiplication. Consider the polynomials $x^2$ and $x^2 + 1$.When we multiply them, $x^2 * (x^2 + 1) = x^4 + x^2$, which is not a degree 2 polynomial, and therefore it is not closed under multiplication and cannot be a ring. Furthermore, $0_R$ is not of degree 2 and therefore is not in the subset.

# Problem 20

Let $D : \mathbb{R}[x] \to \mathbb{R}[x]$ be the derivative map defined by

$$D(a_0 + a_1x + a_2x^2 + ... + a_nx^n) = a_1 + 2a_x + 3a_3x^2 + ... + na_nx^{n-1}$$

Is $D$ a homormorphism of rings? An isomorphism?

### Solution

This is neither a homomorphism of rings nor an isomorphism. We will prove this by showing $D$ does not preserve multiplication. Consider $x^2, x^3 \epsilon \mathbb{R}[x]$. When we multiply them, $x^2 * x^3 = x^5$. Now, we will apply $D$ and multiply them. $D(x^2) * D(x^3) = 2x * 3x^2 = 6x^3 \neq x^5$. Therefore, $D$ does not preserve multiplication and cannot be a homomorphic or isomorphic.

# Problem 13

Prove Theorem 4.10.
**Theorem 4.10**
Let $\mathbb{F}$ be a field and $a(x), b(x), c(x) \epsilon \mathbb{F}[x]$. If $a(x)|b(x)c(x)$ and $a(x)$ and $b(x)$ are relatively prime, then $a(x)|c(x)$.

### Solution

Assume $\mathbb{F}$ be a field and $a(x), b(x), c(x) \epsilon \mathbb{F}[x]$, $a(x)|b(x)c(x)$, and $a(x)$ and $b(x)$ are relatively prime. Then gcd($a(x), b(x)$)=1, by the definition of relatively prime. But then, by Theorem 4.8, this means that for polynomials $u(x), v(x) \epsilon F[x]$,

$$1 = a(x)v(x) + b(x)u(x).$$

Problem 13 continued on next page. . . 

We can multiply this equation by $c(x)$ to get that

$$c(x)a(x)v(x) + c(x)b(x)u(x) = c(x)$$

Since $a(x)|b(x)c(x)$, there exists some $z(x)\epsilon(F)[x]$ such that $a(x)z(x) = b(x)c(x)$. We can substitute this into the above equation to get

$$c(x)a(x)v(x) + a(x)z(x)u(x) = c(x)$$

and we can then factor out $a(x)$ to get

$$a(x)[c(x)v(x) + z(x)u(x)] = c(x)$$

Since $c(x), v(x), z(x), u(x)\epsilon\mathbb{F}[x]$, $a(x)|c(x)$.

# Problem 12

Express $x^4 - 4$ as a product of irreducibles in $\mathbb{Q}[x], \mathbb{R}[x]$, and in $\mathbb{C}[x]$.

**Solution**
First, we will factor this into a product of irreducibles in $\mathbb{C}[x]$. In $\mathbb{C}[x]$,

$$x^4 - 4 = (x - i\sqrt{2})(x + i\sqrt{2})(x - 2)(x + 2)$$

These factors are all irreducible because they are all degree 1, both complex numbers and irrational numbers are in $\mathbb{C}$
In $\mathbb{R}[x]$,

$$x^4 - 4 = (x^2 + 2)(x + \sqrt{2})(x - \sqrt{2})$$

In this case, $(x+\sqrt{2})$ and $(x-\sqrt{2})$ are factors because they are degree 1 with coefficients in the real numbers. $(x + \sqrt{2})$ is only irreducible in $\mathbb{C}[x]$ because it has complex coefficients.
In $\mathbb{Q}[x]$,

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

The first factor is irreducible because if it were not irreducible, it would be reducible in $\mathbb{R}[x]$. The second factor is irreducible because it only factors into polynomials with irrational coefficients, which, by definition, are not in the $\mathbb{Q}$

# Problem 4

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

b For what value of $k$ is $x + 1$ a factor of $x^4 + 2x^3 - 3x^2 + kx + 1$ in $\mathbb{Z}_5[x]$

**Solution**
**a)** For $k = -2$ is $(x - 2)$ a factor of $x^4 - 5x^3 + 5x^2 + 3x + k$. This is simply to solve for because $(x - 2)$ is in the form of a root, so we can evaluate our polynomial at $x = 2$ and solve for $k$.

$$2^4 - 5x^3 + 5x^2 + 3x - k = 0 \Rightarrow 16 - 40 + 20 + 6 = -k \Rightarrow -2 = k$$

**b)** For $k = 3$ is $x + 1$ a factor of $x^4 + 2x^3 - 3x^2 + kx + 1$ in $\mathbb{Z}_5[x]$. Like in part a, since $(x + 1)$ is in the form of a root, we can evaluate our polynomial at $x = -1$ and solve for $k$.

$$(-1)^4 + 2(-1)^3 - 3(-1)^2 + k(-1) + 1 = 0 \Rightarrow 1 - 2 - 3 - k + 1 = 0 \Rightarrow 2 = k + 5 \Rightarrow k = 3$$

# Problem 5

Show that $x - 1_F$ divides $a_nx^n + ... + a_2x^2 + a_1x + a_0$ in $\mathbb{F}[x]$ if and only if $a_0 + ... + a_n = 0_F$.
**Solution**

$\Rightarrow$ Assume that $x - 1_F$ divides $a_nx^n + ... + a_2x^2 + a_1x + a_0$ in $\mathbb{F}[x]$. Then $1_F$ is a root of $a_nx^n + ... + a_2x^2 + a_1x + a_0$, so this means that $a_n1^n + ... + a_21^2 + a_1 + a_0 = 0$. Since 1 to any power is 1, this simplifies to $a_n + ... + a_2 + a_1 + a_0 = 0$

$\Leftarrow$ This proof is simply the above proof in reverse. Assume that $a_0 + ... + a_n = 0_F$ in $\mathbb{F}[x]$. This can be rewritten as $a_01 + ... + a_n1 = 0_F$, or $a_01^0 + ... + a_n1^n = 0_F$. This is the form of a polynomial root evaluated at 1, so $x - 1$ is a factor.

# Problem 14

a Suppose $r, s\epsilon\mathbb{F}$ are roots of $ax^2 + bx + c\epsilon\mathbb{F}[x]$ (with $a \neq 0_F$). Use the Factor Theorem to show that $r + s = -a^{-1}b$ and $rs = a^{-1}c$.

**Solution**
Assume $r, s\epsilon\mathbb{F}$ are roots of $ax^2 + bx + c\epsilon\mathbb{F}[x]$, $a \neq 0_F$. Then, by the Factor Theorem,

$$ax^2 + bx + c = (x - r)(x - s)q(x)$$

We know that $q(x) = 1_F$, because $ax^2 + bx + c$ is degree 2, and we already have two factors. We can express $ax^2 + bx + c$ as it's equivilent monic associate by multiplying by $a^{-1}$. We then have

$$a^{-1}ax^2 + a^{-1}bx + a^{-1}c = (x - r)(x - s)$$

Now, we can multiply the two factors together to get

$$x^2 + a^{-1}bx + a^{-1}c = x^2 - (r - s)x + rs$$

Therefore, since polynomials are equivalent when all of their coefficients are equivealent, we have that $a^{-1}b = r - s$, or $-a^{-1}b = r + s$, and $a^{-1}c = rs$.

# Problem 18

Let $\varphi : \mathbb{C} \to \mathbb{C}$ be an isomorphism of rings such that $\varphi(a) = a$ for each $a\epsilon\mathbb{Q}$ Suppose $r\epsilon\mathbb{C}$ is a root of $f(x)\epsilon\mathbb{Q}[x]$. Prove that $\varphi(r)$ is also a root of $f(x)$.

**Solution**
Since $f$ is a polynomial, we can express it as

$$a_0 + a_1x + \cdots + a_nx^n$$

Now, $r$ is a root, so we can add $r$ to our polynomial by writing it as

$$a_0 + a_1r + \cdots + a_nr^n = 0$$

We can apply $\varphi$ to the entire equation,

$$\varphi(a_0 + a_1r + \cdots + a_nr^n) = \varphi(0)$$

and since it is an isomorphism of rings, it preserves addition and 0, so

$$a_0 + a_1\varphi(r) + \cdots + a_n\varphi(r^n) = 0$$

This is the definition of roots of an equation, and therefore, $\varphi(r)$ is also a root of $f$.

# Problem 19

We say that $a \epsilon \mathbb{F}$ is a multiple root of $f(x) \epsilon \mathbb{F}[x]$ if $(x-a)^k$ is a factor of $f(x)$ for some $k \geq 2$.

a Prove that $a \epsilon \mathbb{R}$ is a multiple root of $f(x) \epsilon \mathbb{R}[x]$ if and only if $a$ is a root of both $f(x)$ and $f'(x)$.

b If $f(x) \epsilon \mathbb{R}$ and if $f(x)$ is relatively prime to $f'(x)$, prove that $f(x)$ has no multiple root in $\mathbb{R}$

**Solution**
**a)**
$\Rightarrow$ Assume that $a \epsilon \mathbb{R}$ is a multiple root of $f(x) \epsilon \mathbb{R}[x]$. By definition of a multiple root, $(x-a)^k$ is a factor of $f, k \geq 2$, and we can write $f(x) = (x-a)^k * g(x)$ for some $g(x) \epsilon \mathbb{F}[x]$. If we differentiate this function, since $k \geq 2$,

$$f'(x) = k(x-a)^{k-1} g(x) + g'(x)(x-a)^k$$
$$f'(x) = (x-a)[k(x-a)^{k-2} g(x) + g'(x)(x-a)^{k-1}]$$

Therefore, $x - a$ is a factor of $f'(x)$, the derivative of $f(x)$, and $a$ is a root of $f'(x)$.

$\Leftarrow$ Assume that $a$ is a root of both $f(x)$ and $f'(x)$. Then we can represent $f(x)$ and $f'(x)$ as

$$f(x) = (x-a)g(x)$$
$$f'(x) = (x-a)h(x)$$

for some $g(x), h(x) \epsilon \mathbb{F}[x]$. We can differntiate the first equation as

$$f'(x) = (x-a)g'(x) + g(x)$$

which we can then substitute into the equation above for $f'(x)$ to get

$$(x-a)h(x) = (x-a)g'(x) + g(x)$$
$$(x-a)h(x) - (x-a)g'(x) = g(x)$$
$$(x-a)[h(x) - g'(x)] = g(x)$$

Finally, we can substitute this equation for $g(x)$ into our first equation and show that

$$f(x) = (x-a) * (x-a)[h(x) - g'(x)]$$
$$f(x) = (x-a)^2 [h(x) - g'(x)]$$

Therefore, a is a multiple root of $f(x)$.

**b)**
Assume that $f(x) \epsilon \mathbb{R}$ is relatively prime to $f'(x)$ and that $f(x)$ and $f'(x)$ have a multiple root. Since they have a multiple root, from part a we can write them as

$$f(x) = (x-a)g(x)$$
$$f'(x) = (x-a)h(x)$$

for some $g(x), h(x) \epsilon \mathbb{F}[x]$. But this implies that they have a common factor, $x - a$, a contradiction. Therefore, $f(x)$ and $f'(x)$ cannot have a multiple root. for some $g(x), h(x) \epsilon \mathbb{F}[x]$.