Math 531 Homework 8

Theo Koss

April 2021

1 Section 4.1

- Problem 1: Let $f(x), g(x), h(x) \in F[x]$. Show that the following hold:

  (a) If $g(x) \,|\, f(x)$, and $h(x) \,|\, g(x)$, then $h(x) \,|\, f(x)$.
  Since $g(x) \,|\, f(x)$, it follows that $f(x) = g(x)\, a(x)$ for some $a(x) \in F(x)$. Similarly, $g(x) = h(x)\, b(x)$, for some $b(x) \in F(x)$. Thus, $f(x) = h(x)\, b(x)\, a(x)$, and since $b(x)\, a(x) \in F(x)$, this shows $h(x) \,|\, f(x)$.

  (b) If $h(x) \,|\, f(x)$, and $h(x) \,|\, g(x)$, then $h(x) \,|\, (f(x) \pm g(x))$.
  Since $h(x) \,|\, f(x)$ and $h(x) \,|\, g(x)$, $f(x) = h(x)\, a(x)$ and $g(x) = h(x)\, b(x)$. Then $(f(x) + g(x)) = h(x)\,(a(x) + b(x))$, thus $h(x) \,|\, (f(x) + g(x))$. And $(f(x) - g(x)) = h(x)\,(a(x) - b(x))$ so $h(x) \,|\, (f(x) - g(x))$, therefore $h(x) \,|\, (f(x) \pm g(x))$.

  (c) If If $g(x) \,|\, f(x)$, then $g(x) \cdot h(x) \,|\, f(x) \cdot h(x)$.
  Since $g(x) \,|\, f(x)$, $f(x) = g(x)\, a(x)$. Then $f(x) \cdot h(x) = g(x)\, a(x)\, h(x)$, thus, $g(x) \cdot h(x) \,|\, f(x) \cdot h(x)$.

  (d) If $g(x) \,|\, f(x)$ and $f(x) \,|\, g(x)$, then $f(x) = kg(x)$ for some $k \in F$.
  Since $g(x) \,|\, f(x)$, $f(x) = g(x)\, a(x)$, and since $f(x) \,|\, g(x)$, $g(x) = f(x)\, b(x)$.

- Problem 5: Over the given field F, write $f(x) = q(x)\,(x - c) + f(c)$ for:

  (a) $f(x) = 2x^3 + x^2 - 4x + 3; c = 1; F = \mathbb{Q}$.

$$f(x) - f(1) = \left(2x^3 + x^2 - 4x + 3\right) - (2 + 1 - 4 + 3)$$

$$= \left(2x^3 + x^2 - 3\right) + (4x - 4)$$
$$= (x-1)\left(2x^2 + 3x + 3\right) + 4(x-1)$$
$$\left(2x^2 + 3x + 7\right)(x-1)$$

Thus $f(x) = (2x^2 + 3x + 7)(x-1) + 2$.

(b) $f(x) = x^3 - 5x^2 + 6x + 5; c = 2; F = \mathbb{Q}$.

$$f(x) - f(2) = \left(x^3 - 5x^2 + 6x + 5\right) - (8 - 20 + 12 + 5)$$
$$= \left(x^3 - 5x^2 + 12\right) + (6x - 12)$$
$$= (x-2)\left(x^2 - 3x - 6\right) + 6(x-2)$$
$$= \left(x^2 - 3x\right)(x-2)$$

Thus $f(x) = (x^2 - 3x)(x-2) + 5$.

(c) $f(x) = x^3 + 1; c = 1; F = \mathbb{Z}_3$.

$$f(x) - f(1) = \left(x^3 + 1\right) - (1+1)$$
$$= x^3 - 1 = (x-1)\left(x^2 + x + 1\right)$$

Thus $f(x) = (x^2 + x + 1)(x-1) + 2$

(d) $f(x) = x^3 + 2x + 3; c = 2; F = \mathbb{Z}_5$.

$$f(x) - f(2) = \left(x^3 + 2x + 3\right) - \underbrace{(8 + 4 + 3)}_{\equiv 0 \mod 5}$$
$$= \left(x^2 + 2x + 6\right)(x-2)$$

Thus $f(x) = (x^2 + 2x + 6)(x-2)$

- Problem 15: Show that the set of matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a field under the operations of matrix addition and multiplication.

  Proof. Call this set S, and consider the elements of this set, $\alpha = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $\beta = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$, and $\gamma = \begin{bmatrix} e & f \\ -f & e \end{bmatrix}$ To show this is a field, we N2S:

1. Closure under addition and multiplication.
2. Associativity of matrix addition and multiplication.
3. Commutativity of matrix addition.

Numbers 1-3 are clearly true with this set. Therefore we must only show

1. Commutativity of matrix mulitplication.
   $\alpha\beta = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} \in S$, $\beta\alpha = \begin{bmatrix} ca-db & da+cb \\ -cb-da & -db+ca \end{bmatrix} \in S$, since $\alpha\beta = \beta\alpha \quad \forall \alpha, \beta \in S$, matrix multiplication on this set is commutative.
2. Distributivity of multiplication over addition.
   N2S, $\alpha\left(\beta+\gamma\right) = \alpha\beta + \alpha\gamma$, $\forall \alpha, \beta, \gamma \in S$.
   $$\alpha\left(\beta+\gamma\right) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \left(\begin{bmatrix} c+e & d+f \\ -d-f & c+e \end{bmatrix} \right)$$
   $$= \begin{bmatrix} a\left(c+e\right)+b\left(-d-f\right) & a\left(d+f\right)+b\left(c+e\right) \\ -b\left(c+e\right)+a\left(-d-f\right) & -b\left(d+f\right)+a\left(c+e\right) \end{bmatrix}$$
   $$\alpha\beta+\alpha\gamma = \left(\begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} \right) + \left(\begin{bmatrix} ae-bf & af+be \\ -be-af & -bf+ae \end{bmatrix} \right)$$
   $$= \begin{bmatrix} a\left(c+e\right)+b\left(-d-f\right) & a\left(d+f\right)+b\left(c+e\right) \\ -b\left(c+e\right)+a\left(-d-f\right) & -b\left(d+f\right)+a\left(c+e\right) \end{bmatrix}$$
   Therefore $\alpha\left(\beta+\gamma\right) = \alpha\beta + \alpha\gamma$, $\forall \alpha, \beta, \gamma \in S$. As required.
3. Existence of identity elements for addition and multiplication.
   Additive identity, "0" $\in S = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Multiplicative identity, "1" $\in S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
4. Existence of additive inverses.
   $\forall \alpha = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in S$, $\exists -\alpha = \begin{bmatrix} -a & -b \\ b & -a \end{bmatrix} \in S$.
5. Existence of multiplicative inverses.
   $\forall \alpha = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in S$, $\exists \alpha^{-1} = \frac{1}{det(\alpha)} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in S$, and $det\left(\alpha\right) = 0$ iff $a, b = 0$, which is the additive identity, therefore this is always defined.

QED

2 Section 4.2

- Problem 3: Find the greatest common divisor of $f(x)$ and $f'(x)$, over $\mathbb{Q}$.

  (a) $f(x) = x^4 - x^3 - x + 1 = (x-1)^2(x+1)$.
  $f'(x) = 4x^3 - 3x^2 - 1 = (x-1)(2x-1)(2x+1)$.
  $\gcd(f(x), f'(x) = (x-1))$.

  (b) $f(x) = x^3 - 3x - 2 = (x+1)(x+1)(x-2)$.
  $f'(x) = 3x^2 - 3 = 3(x+1)(x-1)$.
  $\gcd(f(x), f'(x)) = (x+1)$.

  (c) $f(x) = x^3 + 2x^2 - x - 2 = (x+2)(x+1)(x-1)$.
  $f'(x) = \underbrace{3x^2 + 4x - 1}_{\text{irreducible}}$
  $\gcd(f(x), f'(x)) = 1$. ?

  (d) $f(x) = x^4+2x^3+3x^2+2x+1$ is irreducible, therefore $\gcd(f(x), f'(x)) = 1$.

- Problem 11: Find the irreducible factors of $x^6 - 1$ over $\mathbb{R}$.
  Useful equations:

$$a^2 - b^2 = (a+b)(a-b) \tag{1}$$

$$a^3 - b^3 = (a-b)\left(a^2 + b^2 + ab\right) \tag{2}$$

$$a^3 + b^3 = (a+b)\left(a^2 + b^2 - ab\right) \tag{3}$$

  Let $f(x) = x^6 - 1$,

$$\begin{aligned} f(x) &= x^6 - 1 \\ &= \left(x^3\right)^2 - (1)^2 \\ &= \left(x^3+1\right)\left(x^3-1\right) \\ &= \left(x^3+1^3\right)\left(x^3-1^3\right) \\ &= (x+1)\left(x^2+1-x\right)(x-1)\left(x^2+1+x\right) \\ &= (x+1)(x-1)\left(x^2-x+1\right)\left(x^2+x+1\right) \end{aligned}$$

  This cannot be factorized further with real coefficients.

- Problem 17: Show that for any real number $a \neq 0$, the polynomial $x^n - a$ has no multiple roots in $\mathbb{R}$.

  Proof. Assume, for sake of contradiction, that f has a multiple root, and let $\beta \in \mathbb{R}$ be that root. Then $f(\beta) = 0$, $f'(\beta) = 0$. Plugging in, we see:

  $$f(\beta) = 0 \implies \beta^n - a = 0 \implies \beta^n = a \tag{1}$$

  And

  $$f'(\beta) = 0 \implies n\beta^{n-1} = 0 \tag{2}$$

  and since $n \neq 0$, this means $\beta = 0$, and by (1), $\beta^n = a$ and therefore $a = 0$. $\lightning$ QED