Sabbir Ahmed
DATE: May 1, 2018
MATH 407: HW 12

4.1 **1** Let $f(x)$, $g(x)$, $g(x) \in F[x]$. Show that the following properties hold.

c If $g(x) \mid f(x)$, then $g(x) \cdot h(x) \mid f(x) \cdot h(x)$.

Pf. Since $g(x) \mid f(x)$, then by definition $f(x) = q(x)g(x)$, $q(x) \in F[x]$

Then,

$$\begin{aligned} f(x)h(x) &= q(x)g(x)h(x) \\ &= q(x)(g(x)h(x)) \\ &\implies g(x)h(x) \mid f(x)h(x) \end{aligned}$$ □

d If $g(x) \mid f(x)$ and $f(x) \mid g(x)$, then $f(x) = kg(x)$ for some $k \in F$.

Pf. Since $g(x) \mid f(x)$, then by definition $f(x) = q(x)g(x)$, $q(x) \in F[x]$

And similarly, since $f(x) \mid g(x)$, then by definition $g(x) = r(x)f(x)$, $r(x) \in F[x]$

Therefore,

$$\begin{aligned} \deg(f(x)) &= \deg(q(x)) + \deg(g(x)) \\ \implies \deg(f(x)) &\le \deg(g(x)) \end{aligned}$$

And,

$$\begin{aligned} \deg(g(x)) &= \deg(r(x)) + \deg(f(x)) \\ \implies \deg(g(x)) &\le \deg(f(x)) \end{aligned}$$

Therefore, since $\deg(f(x)) = \deg(g(x))$

and $\deg(q(x)) = \deg(r(x)) = 0$, then $f(x) = kg(x)$ □

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

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

Pf. Since $f(x = c = 2) = (2)^3 - 5(2)^2 + 6(2) + 5 = 5$

Then,

$$\begin{aligned} f(x) - f(c) &= (x^3 - 5x^2 + 6x + 5) - 5 \\ &= x^3 - 5x^2 + 6x \end{aligned}$$

$$= (x^2 - 3x)(x - 2)$$

Therefore, $f(x) = (x^2 - 3x)(x - 2) + 5$ $\square$

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

Pf. Since $f(x = c = 2) = (2)^3 + 2(2) + 3 = 15 \equiv 0 \pmod{\mathbb{Z}_5}$

Then,

$$\begin{aligned} f(x) - f(c) &= (x^3 + 2x + 3) - 0 \\ &= x^3 + 2x + 3 \\ &= (x^2 - x + 3)(x + 1) \end{aligned}$$

Therefore, $f(x) = (x^2 - x + 3)(x + 1)$ $\square$

6 Let p be a prime number. Find all roots of $x^{p-1} - 1$ in $\mathbb{Z}_p$.

Pf. By Fermat's little theorem, for any prime p and x such that $p \nmid x$,

$$x^{p-1} \equiv 1 \pmod{p}$$

Since $\{0, 1, 2, \ldots, p-1\} \in \mathbb{Z}_p$, and there are no elements in $\mathbb{Z}_p$ that divides p,
then $x^{q-1} \equiv 1 \pmod{p}$ for all $q (\neq p) \in \mathbb{Z}_p$ Therefore, all of $\mathbb{Z}_p$ are roots of the polynomial $\square$

7 Show that if c is any element of the field $\mathbb{F}$ and $k > 2$ is an odd integer, then $x + c$ is a factor of $x^k + c^k$.

Pf. By the remainder theorem, if $f(x) \in F[x]$ is a non-zero polynomial, and $c \in F$,
then $\exists\, q(x) \in F[x]$ such that $f(x) = q(x)(x - c) + f(c)$
Since $k > 2$ is odd, $f(-c) = f(x = -c) = (-c)^k + c^k = 0$ $\square$

11 Show that the set $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ is closed under addition, subtraction, multiplication, and division.

Pf. Let $x, y \in \mathbb{Q}(\sqrt{3})$, so $x = a_1 + b_1\sqrt{3}$, $y = a_2 + b_2\sqrt{3}$
Addition,

$$\begin{aligned} x + y &= a_1 + b_1\sqrt{3} + a_2 + b_2\sqrt{3} \\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{3} \end{aligned}$$

$$
\begin{aligned}
&\text{if } c = a_1 + a_2,\ d = b_1 + b_2 \in \mathbb{Q} \\
&\implies c + d\sqrt{3} \in \mathbb{Q}
\end{aligned}
$$

Subtraction,

$$
\begin{aligned}
x - y &= a_1 + b_1\sqrt{3} - a_2 + b_2\sqrt{3} \\
&= (a_1 - a_2) + (b_1 - b_2)\sqrt{3} \\
&\text{if } c = a_1 - a_2,\ d = b_1 - b_2 \in \mathbb{Q} \\
&\implies c + d\sqrt{3} \in \mathbb{Q}
\end{aligned}
$$

Multiplication,

$$
\begin{aligned}
x \cdot y &= (a_1 + b_1\sqrt{3}) \cdot (a_2 + b_2\sqrt{3}) \\
&= a_1a_2 + a_1b_2\sqrt{3} + b_1\sqrt{3}a_2 + b_1\sqrt{3}b_2\sqrt{3} \\
&= a_1a_2 + a_1b_2\sqrt{3} + b_1a_2\sqrt{3} + 3b_1b_2 \\
&= (a_1a_2 + 3b_1b_2) + (a_1b_2\sqrt{3} + b_1a_2\sqrt{3}) \\
&= (a_1a_2 + 3b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{3} \\
&\text{if } c = a_1a_2 + 3b_1b_2,\ d = a_1b_2 + b_1a_2 \in \mathbb{Q} \\
&\implies c + d\sqrt{3} \in \mathbb{Q}
\end{aligned}
$$

Division,

$$
\begin{aligned}
x \div y &= \frac{(a_1 + b_1\sqrt{3})}{(a_2 + b_2\sqrt{3})} \\
&= \frac{(a_1 + b_1\sqrt{3})(a_2 - b_2\sqrt{3})}{(a_2 + b_2\sqrt{3})(a_2 - b_2\sqrt{3})} \\
&= \frac{(a_1a_2 - a_1b_2\sqrt{3} + a_2b_1\sqrt{3} - 3b_1b_2)}{(a_2^2 - a_2b_2\sqrt{3} + a_2b_2\sqrt{3} + 3b_2^2)} \\
&= \frac{(a_1a_2 - 3b_1b_2) + (a_2b_1 - a_1b_2)\sqrt{3}}{(a_2^2 + 3b_2^2)} \\
&= \frac{(a_1a_2 - 3b_1b_2)}{(a_2^2 + 3b_2^2)} + \frac{(a_2b_1 - a_1b_2)}{(a_2^2 + 3b_2^2)}\sqrt{3} \\
&\text{if } c = \frac{(a_1a_2 - 3b_1b_2)}{(a_2^2 + 3b_2^2)},\ d = \frac{(a_2b_1 - a_1b_2)}{(a_2^2 + 3b_2^2)} \in \mathbb{Q} \\
&\implies c + d\sqrt{3} \in \mathbb{Q}
\end{aligned}
$$

$\square$

13 Show that the set of matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where $a, b \in \mathbb{R}$, is a field under the operations of matrix addition and multiplication.

Pf. Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in M$

To prove closure,

$$A + B = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

$$= \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} \in M$$

And,

$$AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

$$= \begin{bmatrix} ac-bd & ad+bc \\ -(bc+ad) & ac-bd \end{bmatrix} \in M$$

To prove that multiplication is commutative,

$$AB = \begin{bmatrix} ac-bd & ad+bc \\ -(bc+ad) & ac-bd \end{bmatrix}$$

$$= \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

$$= BA$$

To prove the existence of the additive identity element, let $e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ such that $A + e = e + A = A$

Since,

$$A + e = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

$$= A$$

To prove the existence of the multiplicative identity element, let $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ such that $Ae = eA = A$

Since,

$$\begin{aligned} A + e &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \\ &= A \end{aligned}$$

To prove the existence of additive inverse elements, let $-A = \begin{bmatrix} -a & -b \\ b & -a \end{bmatrix}$ such that $A + (-A) = (-A) + A = e$

If A is non-zero, then it's determinant $a^2 + b^2 \neq 0$

Therefore

$$\begin{aligned} \det(-A) &= \frac{1}{aa - (-b)b} \begin{bmatrix} -a & -b \\ b & -a \end{bmatrix} \\ &= \frac{1}{a^2 + b^2} \begin{bmatrix} -a & -b \\ b & -a \end{bmatrix} \in M \end{aligned}$$ □

17 Let $(x_0, y_0), (x_1, y_1), (x_2, y_2)$ be points in the Euclidean plane $\mathbb{R}^2$ such that x_0, x_1, x_2 are distinct. Show the formula

$$f(x) = \frac{y_0(x - x_1)(x - x_2)}{(x_0 - x_1)(x_0 - x_2)} + \frac{y_1(x - x_0)(x - x_2)}{(x_1 - x_0)(x_1 - x_2)} + \frac{y_2(x - x_0)(x - x_1)}{(x_2 - x_0)(x_2 - x_1)}$$

defines a polynomial $f(x)$ such that $f(x_0) = y_0$, $f(x_1) = y_1$, and $f(x_2) = y_2$.

Pf.

$$\begin{aligned} f(x) &= \frac{y_0(x - x_1)(x - x_2)}{(x_0 - x_1)(x_0 - x_2)} + \frac{y_1(x - x_0)(x - x_2)}{(x_1 - x_0)(x_1 - x_2)} + \frac{y_2(x - x_0)(x - x_1)}{(x_2 - x_0)(x_2 - x_1)} \\ &= \frac{\begin{array}{l} y_0(x - x_1)(x - x_2)(x_1 - x_2) \\ \quad - y_1(x - x_0)(x - x_2)(x_0 - x_2) + y_2(x - x_0)(x - x_1)(x_0 - x_1) \end{array}}{(x_0 - x_1)(x_0 - x_2)(x_1 - x_2)} \end{aligned}$$

$$= \frac{\begin{array}{l} y_0(x^2 - x_1x - x_2x + x_1x_2)(x_1 - x_2) \\ \quad - y_1(x^2 - x_0x - x_2x + x_0x_2)(x_0 - x_2) + y_2(x^2 - x_0x - x_1x + x_0x_1)(x_0 - x_1) \end{array}}{(x_0 - x_1)(x_0 - x_2)(x_1 - x_2)}$$

$$= \frac{\begin{array}{r} x^2(y_0(x_0 - x_1) - y_1(x_0 - x_2) + y_2(x_1 - x_2)) + x(-y_0(x_0^2 - x_1^2) + y_1(x_0^2 - x_2^2) - y_2(x_1^2 - x_2^2)) \\ + x_1x_2y_0(x_0 - x_1) - x_0x_2y_1(x_0 - x_2) + x_0x_1y_2(x_1 - x_2)) \end{array}}{(x_0 - x_1)(x_0 - x_2)(x_1 - x_2)}$$

Therefore, $f(x)$ is defined as a polynomial

And,

$$f(x_0) = \frac{y_0(x_0 - x_1)(x_0 - x_2)}{(x_0 - x_1)(x_0 - x_2)} + \frac{y_1(x_0 - x_0)(x_0 - x_2)}{(x_1 - x_0)(x_1 - x_2)} + \frac{y_2(x_0 - x_0)(x_0 - x_1)}{(x_2 - x_0)(x_2 - x_1)} = y_0$$

$$f(x_1) = \frac{y_0(x_1 - x_1)(x_1 - x_2)}{(x_0 - x_1)(x_0 - x_2)} + \frac{y_1(x_1 - x_0)(x_1 - x_2)}{(x_1 - x_0)(x_1 - x_2)} + \frac{y_2(x_1 - x_0)(x_1 - x_1)}{(x_2 - x_0)(x_2 - x_1)} = y_1$$

$$f(x_2) = \frac{y_0(x_2 - x_1)(x_2 - x_2)}{(x_0 - x_1)(x_0 - x_2)} + \frac{y_1(x_2 - x_0)(x_2 - x_2)}{(x_1 - x_0)(x_1 - x_2)} + \frac{y_2(x_2 - x_0)(x_2 - x_1)}{(x_2 - x_0)(x_2 - x_1)} = y_2 \qquad \square$$

18 Use Lagrange's interpolation formula to find a polynomial $f(x)$ such that $f(1) = 0$, $f(2) = 1$, and $f(3) = 4$.

Pf. Given Lagrange's interpolation formula,

$$f(x) = \frac{y_0(x - x_1)(x - x_2)}{(x_0 - x_1)(x_0 - x_2)} + \frac{y_1(x - x_0)(x - x_2)}{(x_1 - x_0)(x_1 - x_2)} + \frac{y_2(x - x_0)(x - x_1)}{(x_2 - x_0)(x_2 - x_1)}$$

With $x_0 = 1$, $x_1 = 2$, and $x_2 = 3$, and $y_0 = 0$, $y_1 = 1$, and $y_2 = 4$

$$\begin{aligned} f(x) &= \frac{0(x-2)(x-3)}{(1-2)(1-3)} + \frac{1(x-1)(x-3)}{(2-1)(2-3)} + \frac{4(x-1)(x-2)}{(3-1)(3-2)} \\ &= -(x-1)(x-3) + 2(x-1)(x-2) \\ &= x^2 - 2x + 1 \end{aligned} \qquad \square$$